System security lab 2

In this week we will continue to work with the scenario from lab 1, however we will use different exploits.

Were gonna ‘write’ an exectutionable, by making a batch file and convert it into an .exe

To do this I’m gonna use bat2exe which edge does say ‘may be malicious’ but windows allows me to download it.

I’ve already written a batch script to make a new user, so I’m going to turn that into an .exe and call it Common.exe, because the unquoted path service is going to look for:

* Disc C, is there a .exe?
* Program.. is there a program.exe?
* Files/ Common… is there a common.exe? ((HIT)
* Etc..

Therefore when I put the common.exe in the program files > unquoted path service, but before common files, it will hit on my common.exe

Then I restart the service and voila, my new account is there.

We’re gonna download Sysinternals now to see if we can look into the permissions to stop/start services.

I’m gonna run ‘start accesschk.exe -uwvqc “normaluser” \*

Which returns: RW daclsvc  
query status, query config, change config, interrogate, enumerate dependents, start, stop, readcontrol

This shows us that we have control over DACL service, so I’m going to run;

Sc config dalcsvc binpath= “cmd /c cmd.exe /c net user /add misterbean L3tm3!n && net localgroup administrators misterbean /add”

Then, refresh and start the DACL service and head to computer management, which shows me the user misterbean has been added.

The next step would be defense evasions, so we’d have to find a way to disable antivirus or circumvent it, this could be done by adding exclusions in defender. I can log in as my earlier made administrator user my putting .\misterbean as username, so that it puts it on local machine and not ADLAB, my password, and then exclude the whole C:\ folder.

I was able to install mimikatz, and then I run privilege::debug, and sekurlsa::logonpasswords. I looked up on google how I could crack ntml hashes and such, but found that I can pass the hash using mimikatz. I ran the command sekurlsa::pth /user:Administrator /domain:WIN10CLIENT /ntlm:af992895db0f2c42a1bc96546e92804a which opened a CMD with system privileges.

Now it’s time to start the admin machine, to check if the hash // password is getting re-used. Which is a common mistake a lot of people have.

Now, lets head to the administrator cmd I have opened using passthehash, I can run dir [\\192.168.56.30\c$](file:///\\192.168.56.30\c$) which returns the directory of the admin machine. Because we can do a directory listing of this specific share (the $ means its hidden) it means we are administrator, because only the administrator can access this. It also means the admin password is reused across the domain.

From this administrator cmd, I can run PsExec. I’m gonna run PsExec [\\192.168.56.30](file:///\\192.168.56.30) cmd which opens up the CMD line, when I type Whoami it shows I’m win10adm\administrator, which means I’m now on the CMD on the admin machine.

This also means I can use psexec to do a lot more things from the remote machine

Now we have to figure out how to run Procmon as admin, so that we can run dllsvc to do a dll hijack, and research dll hijacking. I can start Procmon from the new system CMD.

(and, do some priv esc and make us be able to have an admin window open)