**Scenario:**

Inside job

**Description:**

Megacorp (a very large company) have recently purchased a number of SMEs (smallmedium enterprises). Megacorp are very risk-averse and take their security posture very seriously. They are performing a number of in-parallel security assessments.

Your task is to assess the “insider threat” scenario in a red-team exercise. Yu will discover and exploit all the security issues you are able to find. Your goal is to move from low privileged domain user to demonstrating control over the Active Directory environment, while uncovering as many exploitation paths as possible.

There are nomarksforfinishingfirst,yourclientexpectsathoroughexaminationoftheenvironment.

**Rules of engagement:**

You may use any tools or techniques you can find, as long as you obey the following rules:

1. You may not shutdown, reboot, crash or otherwise disrupt the domain controller.

2. You may not log on locally to Tom’s admin workstation - you may connect over the network.

3. You may not shutdown, reboot, crash (etc) the admin workstation.

4. You may not kick the admin out of his logged-on session.

We do not expect to be perfectly stealthy, but the above actions are creating too much noise!

**Writeup**

Going into the client machine and navigating to settings>apps, I can find a few installed apps. In this list I can find Angry IP Scanner, Oracle VM virtualbox, Remote Desktop connection & Remote mouse version 4.602.

I’m going to open CMD, to check if I can access it, and/or run it in admin mode. I can open it, but not as administrator.

To run Powershell, regualrly and as admin, it either says its blocked or it asks me for the admin username and password. I tried ‘admin admin’ but to no avail. It does seem like Powershell x86 isn’t blocked, but the admin version is still blocked.

I’m gonna open up cmd and run Ipconfig /all, just to find out what IP my device is and what other info I can find. Here I see that the DNS server for adapter 1 and 2 are 192.168.56.5 and 192.168.56.10. I also dee the default gateway is 192.168.56.1. My IPv4 adress for adapter 1 and 2 are 10.0.3.15 and 192.168.56.40.

The primary DNS suffix is ADLAB.local

I ran Nslookup, that gave me pi.hole as default server, with address 192.168.10.5.

I’m gonna launch Angry IP Scanner, and scan the 192.168.56.x IP range (0 – 255) and see what it comes up with. It shows me that .1(gateway), .10(dns, WIN2019DC so the domain controller) .30(WIN10ADM, so the admin account), .40 (me), and .100

Besides that, I can navigate to [\\Win2019DC](file:///\\Win2019DC) and [\\Win10ADM](file:///\\Win10ADM) in the file explorer. Win10ADM is empty, but Win2019DC has 2 folders, called NETLOGON and SYSVOL. In the Sysvol file there’s a shortcut to ‘adlab.local’ which have the policies and scripts inside. The scripts folder is empty, but the policies folder has 5 policies. There doesn’t seem to be much interesting inside.

It also seems like the windows machine I’m on isn’t fully up to date, it still wants the 2024-08 update for windows 10 version 22h2 (etc).

I can also download stuff from the internet, but when I install it it’ll ask for an admin password. It does seem like (for example chrome) It will install it anyways.

I’m also going to look at the current services, I don’t have much knowledge about windows services but there are some things running such as Workstation, Remote management, Connection manager, remote access control manager etc. There’s also services without description that are all running on local system. These are DACL service, DLL Hijack service, File permissions service, Insecurity Registry Service, Remote mouse service and Unquoted path service.

I’m also going to run net user and then net user administrator, this gives me a little bit of information like the password being changeable since 5-9-24, but that’s about it. With net localgroup administrators it shows me theres ADLAB/Domain admins, ADLAB/IT Admins and Administrator.

In the scheduled tasks, there’s only the ones that are running locally, I can access System32, but I cant open the Tasks folder because it requires the administrator password. When I go back to the Windows folder, I can open the Tasks Migrated folder, which is readable. So now I can see all tasks on the system, not just the local ones.

There is a task called Pinger.bat, created my Administrator. Description; “ping the domain”. It runs the batch file when anyone logs on.

The batch file is in C:/Temp, which I can open. It contains @echo off, REM setlocal enabledelayedexpansion, that just sets date/time and then pings adlab.local. However, when trying to edit it, it does’t allow us to. We rename the Temp folder and create a new one, which would allow us to create out own pinger.bat, that we can let run any command on logon with admin access. Like, creating a user.

To do this, I’m going to rename temp to temp.old, then create a new temp folder and make a pinger.bat, and give it the “net user helpdesk H3lpD3sk! /add >> net localgroup administrators helpdesk /add”. When I log out and in, and head to computer management > users and local groups, I can find the new helpdesk user.

Now that I technically have access to an admin account, I could look a little further and try to see if I can use it in any possible way.

I checked the Remote mouse app, and it gives me the option to select an ‘image transfer folder’, in which I could navigate to anywhere such as the system32 folder. IF I open system32 though this folder, It opens as administrator system32. If I run ‘whoami’, it shows nt authority\system.

Remote mouse has a CVE that leads to privilege escalation, CVE-2021-35448.

Because remote mouse is one of the services without description, it might mean that the other services without descriptions might also be vulnerable.

There’s also a service called Administrative Task Assist, which runs as .\Administrator. When I check properties, there is also a password saved.

When I go into the registry editor, I can head to Computer\HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\regsvc, in which I’m able to change the Imagepath and set the data to a cmd command, like cmd.exe /c curl parrot.live

There’s also a service called Unquoted path service. When I check the file location of this and check the properties, it shows that it doesn’t have any quoted to direct to. Just C:\Programfiles\Unquoted path service\Common Files\unquotedpathservice.exe

The way windows searches for executables when theres no quoted or spaces, it will just look for the executable and tries to find the .exe, so I could create my own unquotedpathservice.exe within the unquoted path service (outside of the common files folder) which means windows will automatically hit on my version of the executable.

I’m just going to use my .bat file and convert it to .exe using an online converter, rename it and drop it in the main folder.

**HOMEWORK**

Make my own priv escalation exploit (not services or remote mouse)