Hyper-V Administrators

The Hyper-V Administrators group has full access to all Hyper-V features. If Domain Controllers have been virtualized, then the virtualization admins should be considered Domain Admins. They could easily create a clone of the live Domain Controller and mount the virtual disk offline to obtain the NTDS.dit file and extract NTLM password hashes for all users in the domain.

It is also well documented on this blog, that upon deleting a virtual machine, vmms.exe attempts to restore the original file permissions on the corresponding .vhdx file and does so as NT AUTHORITY\SYSTEM, without impersonating the user. We can delete the .vhdx file and create a native hard link to point this file to a protected SYSTEM file, which we will have full permissions to.

If the operating system is vulnerable to CVE-2018-0952 or CVE-2019-0841, we can leverage this to gain SYSTEM privileges. Otherwise, we can try to take advantage of an application on the server that has installed a service running in the context of SYSTEM, which is startable by unprivileged users.

Target File

An example of this is Firefox, which installs the Mozilla Maintenance Service. We can update this exploit (a proof-of-concept for NT hard link) to grant our current user full permissions on the file below:

Target File

C:\Program Files (x86)\Mozilla Maintenance Service\maintenanceservice.exe

Taking Ownership of the File

After running the PowerShell script, we should have full control of this file and can take ownership of it.

Taking Ownership of the File

C:\htb> takeown /F C:\Program Files (x86)\Mozilla Maintenance Service\maintenanceservice.exe

Starting the Mozilla Maintenance Service

Next, we can replace this file with a malicious maintenanceservice.exe, start the maintenance service, and get command execution as SYSTEM.

Starting the Mozilla Maintenance Service

C:\htb> sc.exe start MozillaMaintenance

Note: This vector has been mitigated by the March 2020 Windows security updates, which changed behavior relating to hard links.