**Mount VHDX/VMDK**

During our enumeration, we will often come across interesting files both locally and on network share drives. We may find passwords, SSH keys or other data that can be used to further our access. The tool [Snaffler](https://github.com/SnaffCon/Snaffler) can help us perform thorough enumeration that we could not otherwise perform by hand. The tool searches for many interesting file types, such as files containing the phrase "pass" in the file name, KeePass database files, SSH keys, web.config files, and many more.

Three specific file types of interest are .vhd, .vhdx, and .vmdk files. These are Virtual Hard Disk, Virtual Hard Disk v2 (both used by Hyper-V), and Virtual Machine Disk (used by VMware). Let's assume that we land on a web server and have had no luck escalating privileges, so we resort to hunting through network shares. We come across a backups share hosting a variety of .VMDK and .VHDX files whose filenames match hostnames in the network. One of these files matches a host that we were unsuccessful in escalating privileges on, but it is key to our assessment because there is an Active Domain admin session. If we can escalate to SYSTEM, we can likely steal the user's NTLM password hash or Kerberos TGT ticket and take over the domain.

If we encounter any of these three files, we have options to mount them on either our local Linux or Windows attack boxes. If we can mount a share from our Linux attack box or copy over one of these files, we can mount them and explore the various operating system files and folders as if we were logged into them using the following commands.

**Mount VMDK on Linux**

Mount VMDK on Linux

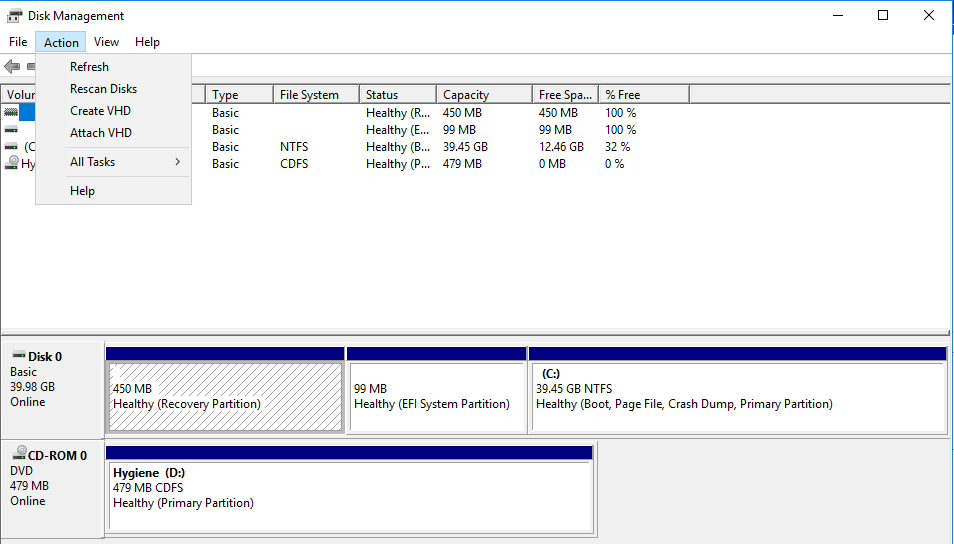
yovecio@htb[/htb]$ guestmount -a SQL01-disk1.vmdk -i --ro /mnt/vmdk

**Mount VHD/VHDX on Linux**

Mount VHD/VHDX on Linux

yovecio@htb[/htb]$ guestmount --add WEBSRV10.vhdx --ro /mnt/vhdx/ -m /dev/sda1

In Windows, we can right-click on the file and choose Mount, or use the Disk Management utility to mount a .vhd or .vhdx file. If preferred, we can use the [Mount-VHD](https://docs.microsoft.com/en-us/powershell/module/hyper-v/mount-vhd?view=windowsserver2019-ps) PowerShell cmdlet. Regardless of the method, once we do this, the virtual hard disk will appear as a lettered drive that we can then browse.



For a .vmdk file, we can right-click and choose Map Virtual Disk from the menu. Next, we will be prompted to select a drive letter. If all goes to plan, we can browse the target operating system's files and directories. If this fails, we can use VMWare Workstation File --> Map Virtual Disks to map the disk onto our base system. We could also add the .vmdk file onto our attack VM as an additional virtual hard drive, then access it as a lettered drive. We can even use 7-Zip to extract data from a .vmdk file. This [guide](https://www.nakivo.com/blog/extract-content-vmdk-files-step-step-guide/) illustrates many methods for gaining access to the files on a .vmdk file.

**Retrieving Hashes using Secretsdump.py**

Why do we care about a virtual hard drive (especially Windows)? If we can locate a backup of a live machine, we can access the C:\Windows\System32\Config directory and pull down the SAM, SECURITY and SYSTEM registry hives. We can then use a tool such as [secretsdump](https://github.com/SecureAuthCorp/impacket/blob/master/impacket/examples/secretsdump.py) to extract the password hashes for local users.

Retrieving Hashes using Secretsdump.py

yovecio@htb[/htb]$ secretsdump.py -sam SAM -security SECURITY -system SYSTEM LOCAL

Impacket v0.9.23.dev1+20201209.133255.ac307704 - Copyright 2020 SecureAuth Corporation

[\*] Target system bootKey: 0x35fb33959c691334c2e4297207eeeeba

[\*] Dumping local SAM hashes (uid:rid:lmhash:nthash)

Administrator:500:aad3b435b51404eeaad3b435b51404ee:cf3a5525ee9414229e66279623ed5c58:::

Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::

DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::

[\*] Dumping cached domain logon information (domain/username:hash)

<SNIP>

We may get lucky and retrieve the local administrator password hash for the target system or find an old local administrator password hash that works on other systems in the environment (both of which I have done on quite a few assessments).