Server 2019 Active Directory vulnerable:

- Active directory is enable.
- User and group are created.
- DNS is also configure.

Now we will make this server vulnerable for active directory attack.

Note: we cannot make vulnerable the server in real world, here we can do this for test and practice purpose.

So move forward.

Create a vulnerable Active Directory that's allowing you to test most of Active Directory attacks in local lab. Supported Attacks Are Abusing ACLs/ACEs, Kerberoasting, AS-REP Roasting, Abuse DnsAdmins, Password in Object Description, User Objects with Default password, Password Spraying, DCSync, Silver Ticket, Golden Ticket, Pass-the-Hash, Pass-the-Ticket and SMB Signing Disabled.

Prerequisites

1. You need to have a Windows Server running in VMware. I had a Windows Server 2019.
2. If you have a Server without an AD in VM, and you don't want to set up the AD manually, you can set it up using the following script.

If you donot configure the active directory copy and paste the below script in windows powershell.

```
Install-ADDSForest -CreateDnsDelegation:$false -DatabasePath "C:\Windows\NTDS" -DomainMode "7" -DomainName "test.local" -DomainNetbiosName "Test" -ForestMode "7" -InstallDns:$true -LogPath "C:\Windows\NTDS" -NoRebootOnCompletion:$false -SysvolPath "C:\Windows\SYSVOL" -Force:$true
```

1. Login to your Domain Controller machine in my case Windows Server 2019.
2. Open the PowerShell in Windows Server 2019.
3. Run the following command to download the script from the GitHub repo.

```
IEX((new-object net.webclient).downloadstring("https://raw.githubusercontent.com/wazehell/vulnerable-AD/master/vulnad.ps1"));
```

Then followed by below command.

Invoke-VulnAD -UsersLimit 100 -DomainName "test.local"

Note: above script I will take from github.

After running above 2 commands you will see hundreds of users in active directory.

Some store their password in description

Some using week passwords and etc.