Vulnerable AD Configuration:

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.

```
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/vulnerableAD/master/vulnad.ps1"));
```

followed by below command.

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